SUPPLEMENTING IT EVENT STANDARDS FOR MISSION ASSURANCE

William Heinbockel
The MITRE Corporation
Bedford, MA

Rosalie McQuaid
The MITRE Corporation
Bedford, MA

ABSTRACT

Computer network defense (CND) capabilities are designed for business efficiency in a static, stable network environment, where network assets are known and the mission of the network rarely varies. Such capabilities do not consider mission needs when identifying and compensating for attacks on assets critical to the current mission. Security awareness remains the same whether the network is carrying redundant inventory data or supporting critical operations. Advanced attackers who may already know the network details, its systems and software, and any mission objectives therefore already have an advantage.

We propose a three-step process to enable migration from the current CND strategy toward one of mission network defense. This transition would lead to better, more adaptable security capabilities by encouraging exchange of mission-related event information. By adopting and extending the Common Event Expression standard to support mission-relevant data, CND systems can begin to monitor their mission environment. Once standardized mission event information becomes available, we can concentrate on developing more adaptive CND capabilities that are better suited to the various mission environments.

INTRODUCTION

Imagine your entire computer network defense (CND) or information assurance (IA) infrastructure automatically reacting to external sensory information. In this scenario, mission-level events, such as an increase in the National Threat Advisory level, would cause each CND capability to modify its behavior to best reflect the mission changes: tighten operating system configurations, deny non-vital network traffic, or issue an alert against a wider range of suspicious activities. The security information and event management (SIEM) correlation engine could consider these mission-level events in its correlations and include them in its final analysis.

Today, CND capabilities are mostly ignorant of higher-level operational tasks, or mission events, and thus perform poorly in dynamic, mission-focused environments. They cannot modify their behaviors and adapt to mission changes: they perform the same way whether the network is idle, under attack, or supporting critical operations. While this may be surprising, since every network serves at least one mission, it is understandable. The target market for CND systems seeks business efficiency – a mission in which systems are dedicated to the same specific tasks and security awareness does not change with the risk. To assure achievement of overarching mission objectives, CND capabilities must begin to utilize mission-relevant data and adapt their behaviors accordingly.

We provide a process, in line with the goals of DoD Directive 3020.40 "Defense Critical Infrastructure Program (DCIP),"[1] to transition our CNDs to better protect the mission objectives. The mission network defense (MND) process is designed as a general and cost-effective approach. The proposed process would permit the creation of more dynamic CND capabilities that can adapt to mission needs. Instead of modifying individual CND capabilities to improve their functioning in a particular mission-focused environment, our process provides both the requisite mission information and guidance on how a system may incorporate such data into its operation. As it is unlikely that future CND capabilities will be able to locate and utilize the heterogeneous data formats specific to each mission, such a process would depend on a standardized method of expressing the requisite mission data.

[1] DoD Directive 3020.40 "Defense Critical Infrastructure Program (DCIP)". [Online] August 19, 2005. http://www.dtic.mil/whs/directives/corres/pdf/302040p.pdf.

978-1-4244-2677-5/08/$25.00 ©2008 IEEE

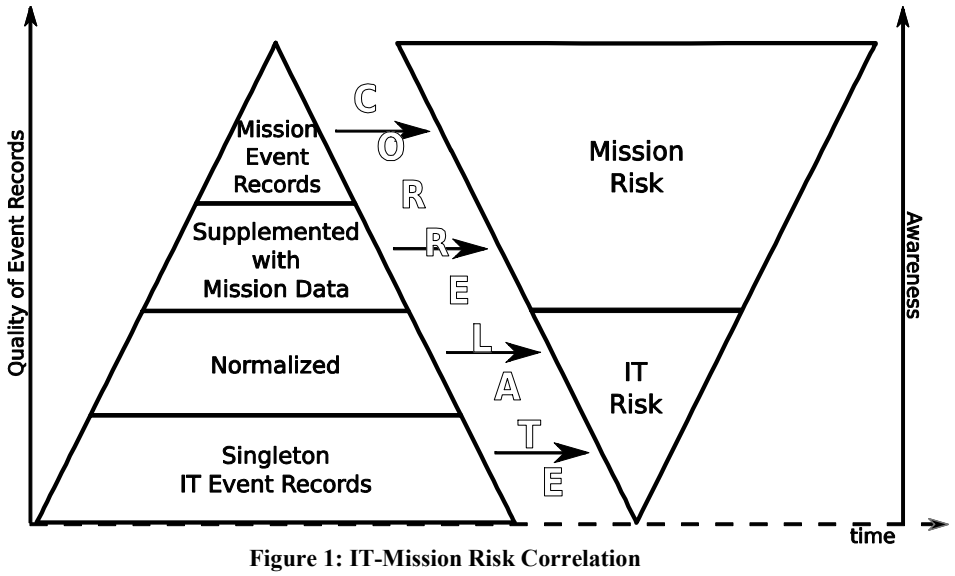

Figure 1: IT-Mission Risk Correlation

The Common Event Expression (CEE™) standard,[2] developed by The MITRE Corporation in collaboration with the NATO Consultation, Command and Control Agency (NC3A), information technology (IT) vendors, and IT administrators, can provide the basis for the MND process. CEE standardizes the representation and exchange of logs from disparate electronic systems. These logs – from operating systems, virus scanners, firewalls, and intrusion detection systems (IDSs) – supply key pieces of information that can be used for computer support, security, or forensic analysis. Most CND infrastructures rely on these logs to identify cyber attacks and improve their security posture. Extending CEE to include mission-relevant data would provide the capability not only to characterize IT events according to mission significance, but also to express events that are entirely mission related. A process based on CEE would enable dynamic, mission-focused behavior in CND systems, while reducing development and deployment costs and avoiding the need to generate and mandate entirely new standards.

TRANSITIONING CND INTO MND

The worlds of IT and missions are merging. While IT is an enabler for missions, many people still perceive little relationship between the two. This is no more evident than in the area of CND: systems protect against IT threats, while people defend against mission threats. As users increase their reliance on the supporting IT infrastructure, mission success depends on the supporting CND infrastructure.

The only way to bridge this gap is to change our perceptions of CND and missions. What is needed is MND – the transition of CND capabilities into the mission environment, with the goal of ensuring the success of the mission. While it is easy to cross-train a soldier in both CND and mission operations, it is much harder to incorporate mission data into CND capabilities, as they have not been developed to be able to handle mission-level information. The capabilities must be able to observe both IT and mission-related events, understand the current IT and mission environments, and adapt their operations to reduce mission risk.

In order to do this, the relation between IT events and their risk must be understood [Figure 1]. Current CND systems are only capable of producing single, heterogeneous IT event records. These inconsistent records severely limit IT awareness. To improve this, the expression of IT event records must be normalized. With standardized IT events, they can begin to be supplemented with mission-related information (e.g., geolocation, personnel data, or system-mission relations) to help calculate the mission impact of IT events. However, to best evaluate mission risk, records of mission events must be made available. Our process utilizes CEE reach the pinnacle IT and mission awareness by improving the quality and availability of event records, evolving today's limited CND capabilities into full MND solutions.

[2] **The MITRE Corporation.** Common Event Expression: CEE, A Standard Log Language for Event Interoperability in Electronic Systems. [Online] 2008. http://cee.mitre.org.

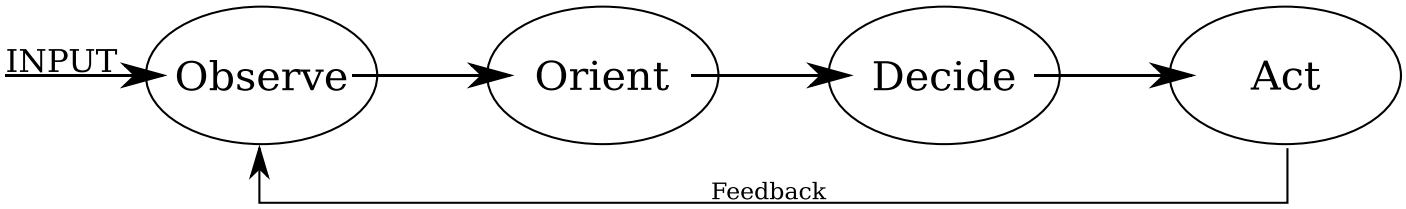

Figure 3: A Simplified Version of Boyd's OODA Loop

This process consists of three steps and is based on the OODA Loop [Figure 2] proposed by Col. John Boyd, USAF (Ret.)[3]. The OODA Loop defines a decision cycle based on the concepts of Observe, Orient, Decide, and Act: *observe* all external and environmental inputs; *orient* these inputs drawing on other knowledge, such as previous experiences; on the basis of this information, *decide* the best option, and *act* on it. Our MND process [Figure 3] focuses on the first three phases of this loop: observe, orient, and decide. Since a commander or other person will make the final decision on all matters involving the mission, we skip the "act" portion.

The first part of the process is to observe environmental inputs. This means that MND capabilities must be aware of their environment. They can observe mission data in two ways: (1) mission-level events and (2) IT events coupled with related mission details. Unfortunately, it is not enough merely to "tell" a product when something changes. Since technology understands syntactics better than semantics, products must be told in a standardized communication format. Our work with the CEE standard for log records provides an ideal basis for representing such mission information.

Second, the systems must be provided with context – knowledge that they can use to supplement the observed inputs. This may be IT- or mission-specific knowledge regarding different mission objectives, operational environments, guidelines, procedures, etc. For certain CND capabilities, such as IDSs, this information might consist of vulnerability reports, suspicious IP blocks, or asset and configuration information. As most of the CND capabilities affected probably already have sufficient IT information, both the IT and mission data have been included in the orientation for completeness.

The final step is the decision phase. As most CND capabilities are already highly specialized, this decision process may be straightforward. If an observed event or event sequence matches one or more of the preset rules, the CND system takes a prescribed action. Other inputs are essentially ignored. For MND capabilities making decisions at the mission level, decisions are more likely to take the form of recommendations to a human operator. For example, a SIEM appliance could correlate IT and mission events and recommend that a specific IP address be blocked at the firewall or that the operator further investigate an event that occurred.

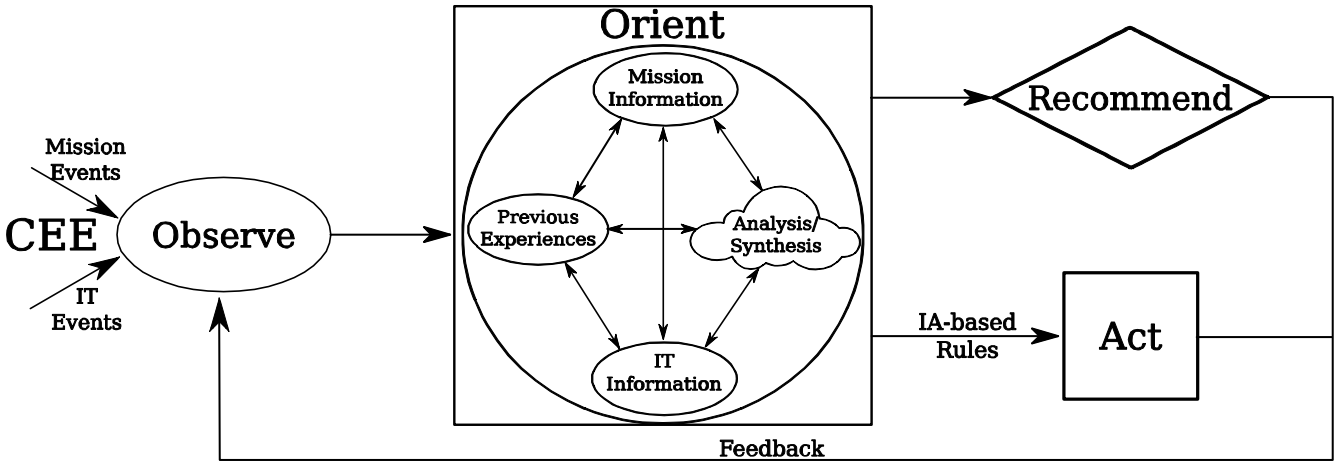

Figure 2: MND Process

[3] **Clark, Donald.** OODA: Observe, Orient, Decide, & Act. [Online] 2004. http://www.nwlink.com/~Donclark/ leadership/ooda.html.

OBSERVING WITH EVENTS VIA CEE

To support MND effectively, all CND capabilities must be able to leverage non-IT events and data. However, since today's concept of CND is restricted to IT, cyber attacks can only be identified by processing disparate events, captured in system logs. CND correlation engines might correlate firewall, anti-virus, and other IT events with IDS alerts in multiple formats. Analysts must expend considerable time to handle even a portion of these heterogeneous events, which range from fairly insignificant network and system scans to critical buffer overflows and remote code execution. They must manually assess mission risk and determine how best to react to ensure mission success.

IMPORTANCE OF LOGS

Logs record one or more events, typically in the context of IT systems. They contain information about what happened, along with details as to the specific users, systems, files, configurations, or resources involved. Logs are sometimes referred to as log files, audit logs, or audit trails. In some cases, logs also cover alerts, alarms, event records, other event logs, event messages, log records, and audit records.

The first signs of trouble in an electronic system appear in the log files. Knowing that computers can react much faster than humans, should we not invest more resources in technology to monitor potential problems and alert analysts about them – especially if those problems could put a mission at risk?

CEE GOALS AND FUNCTIONS

CEE facilitates the transmission, parsing, and understanding of log messages. MITRE is working with its NC3A and industry partners in the CEE effort to standardize IT event logs. The overall effort addresses five related areas necessary for the flexible recording of events in logs and the re-creation of events from logs: transport, syntax, data dictionary, taxonomy, and log recommendations. Such an event standard can not only be used to enhance security and network awareness and improve IA products, but can also serve as a foundation for exchanging mission-relevant data.

CEE breaks the recording and exchanging of logs into four components: the log syntax, event taxonomy, log transport, and logging recommendations.

1. Log Syntax – The syntax is how an event is written in the audit log; it defines the sequence of fields or components. It allows data from the logs to be parsed unambiguously. To maintain consistency and compatibility among the different syntaxes, CEE provides a data dictionary – a collection of event attributes – that is used to describe an event. This dictionary contains the unique syntax identifiers along with their meaning, format, and usage requirements. The dictionary attributes can then be represented in a corresponding text-, XML-, or binary-encoded syntax [Figure 4].
2. Event Taxonomy – The taxonomy specifies the type of event. Think of it as a set of buckets, where each bucket corresponds to a unique event type: user logins, service restarts, network connections, privilege elevations, account creations, etc. Each event log is inherently restricted to record only one event, which must be of a single taxonomic type. By using these "type buckets" when referring to events, CEE enables straightforward log interpretation along with a more scalable log infrastructure.
3. Log Transport – A transport mechanism is required to exchange logs. The transport simply defines how the logs are transmitted. Possible transport options could be in files or via e-mail (SMTP), Syslog, or custom protocols. The transport addresses options such as transit-based encryption and transmission reliability.

```
<?xml version="1.0" ?>
<log event_count="1">
  <event>
    <id> ID001 </id>
    <time> 2008-02-07T16:33:34-06:00
</time>
    <logger>
      <name> kernel </name>
      <pid> 100 </pid>
    </logger>
    <tax_action> denied </tax_action>
    <tax_object> connection </tax_object>
    <tax_status> success </tax_status>
    <end_time> 2008-02-07T22:33:34Z
</end_time>
    <network>
      <device>
        <ip> 10.0.0.1 </ip>
      </device>
      <source>
        <ip> 10.1.1.100 </ip>
        <port> 1659 </port>
      </source>
      <destination>
        <ip> 10.0.0.1 </ip>
        <port> 80 </port>
      </destination>
      <direction> inbound </direction>
      <tcp_flags> SYN FIN </tcp_flags>
      <transport> TCP </transport>
      <proto> IP </proto>
    </network>
  </event>
</log>
```

Figure 4: Example CEE Log in XML

4. Logging Recommendations – The recommendations are a collection of logging best practices. CEE offers guidance to address questions such as: "What are the minimum event types a device should record?" and "What fields should be recorded?" Though not strictly a standard specification, the recommendations represent a necessary and complementary portion of CEE to ensure maximum interoperability.

When events occur, the logging recommendations guide how CEE records them in a log. These recommendations suggest the events and associated details that should be logged by various device types (e.g., operating system, IDS, firewall). The log messages can then be exchanged using a common log transport. Once a message is received, CEE's standard syntax allows machines to quickly parse out relevant data. Finally, CEE's event taxonomy is used to specify the corresponding event type. Without this level of interoperability, achieving optimal awareness of an event becomes an intractable problem as the number of electronic systems and their generated events increases. The only way to overcome this obstacle is through an accepted, industry-wide event expression standard.

EXTENDING CEE TO SUPPORT MND

We believe that the CND correlation engines we rely on for IT event data can also be used to improve mission assurance and assess the overall mission impact of various IT events. This can be done by providing more information in a standardized format, which should lead to improved awareness. Human analysts will quickly experience information overload, but properly configured MND capabilities could easily filter and process millions of standardized event records.

While CEE was developed primarily to address regulatory compliance demands and CND awareness needs, the flexibility and extensibility of CEE can benefit mission-focused environments. A mission-focused CEE extension could extend logs with information that falls outside the scope of IT systems without sacrificing compatibility. Including data such as Global Positioning System (GPS) coordinates, heading, or altitude, or vehicle, unit, or troop identification, would improve event information flows and enhance overall awareness.

Assume that a plane is flying circuits over a battlefield, acting as a communications relay. During one circuit, the crew is retasked to perform a critical radar sweep of a nearby locale and transmit the imagery back to command; this request is also sent as a new CEE mission event to an onboard MND correlation engine. During this time, an IT component necessary to complete the mission (e.g., radio or satellite link, e-mail server, radar imagery system) fails. Again, the failure is immediately recorded as a CEE IT event record and transmitted within the MND infrastructure. Moments after receiving the CEE record from an IDS alerting that a system may be under attack, another CEE IT event is generated indicating the IT system failure. Since an MND capability would incorporate mission context, it would "know" that the system under attack runs the e-mail service on the enclaved platform. The MND capability correlates these three events with other observations and analyzes them against known mission information.

While an inoperable IT component may not pose a large IT risk, the mission risk could be substantial enough to jeopardize the completion of a mission objective. The correlation engine immediately realizes that the failure of the critical IT component will endanger the mission, and promptly alerts the analyst, who, until this point, has wasted no time overseeing the IT infrastructure. The operator receives near-real-time recommendations and risk

```
<?xml version="1.0" ?>
<log>
  <event>
    <name> Radio Link status </name>
    <time> 2008-04-29T14:34:07-05:00 </time>
    <logger>
      <name> radio sensor </name>
    </logger>
    <tax_action> down </tax_action>
    <tax_object> link </tax_object>
    <tax_status> success </tax_status>
    <category> Mission Alert </category>
    <network>
      <name> onboard radio link </name>
      <bandwidth> 50 kbps </bandwidth>
      <capacity> 128 kbps </capacity>
      <radio>
        <name> Radio1 </name>
        <power> 8 </power>
        <band> HF </band>
        <frequency> 10 MHz </frequency>
        <enc_pkg> ID </enc_pkg>
      </radio>
    </network>
    <mission>
      <impact> Radio Comms Problems </impact>
      <fix> Increase Radio1 Power </fix>
    </mission>
    <troop>
      <plane> Tail number </plane>
      <commander> Lt Gen Doe </commander>
      <crew> Crew members </crew>
      <country> United States </country>
    </troop>
  </event>
</log>
```

Figure 5: Mission Data in a CEE XML Log

analysis that draw attention to a potential problem before the threat is even realized. Today's CND infrastructure could correlate the system attack and the services that might be affected. However, it would leave estimation of the mission risk to the analyst.

CEE would also allow use of mission data to forecast potential issues for mission planners or assist operators in responding to problems in their electronic devices. For example, if a radio link continually fails, operators could use information in the CEE record [Figure 5], such as the configured encryption package, GPS locations, weather, and operational frequency band, along with other possible mission logs, to deduce possible causes for the outage more quickly. Going one step further to include external information regarding the current mission tasking (timeline, locations, troops, required resources, etc.) could even allow a MND system to recommend the best mitigation strategy, e.g., increasing power, using additional radios, or switching to another communications method.

CEE is flexible enough that it can be used to represent entire mission-level events. The current CEE taxonomy for describing IT events could easily be extended to include terminology specific to missions. By developing mission sensors that log mission-specific data and events, and adding logging capabilities to current mission planning and coordination systems, operators can leverage logs to cause systems to modify their behaviors. With these added events, the MND infrastructure can be notified when the mission, or any related detail, changes.

CONCLUSION

Given their limited human and IT resources, mission environments must make efficient use of all available information. Humans should not have to spend their time making assessments that CND capabilities could provide. By explicitly describing the possible mission objectives that IT systems may support, and mapping system capabilities to these objectives, MND can enable transient security posturing and improved mitigation. Even if systems become more resilient against attacks, it is impossible to secure everything. Systems can still fail for any number of reasons, such as misconfigurations, attacks, or hardware malfunctions. Including standardized and accepted MND attributes (e.g., mission needs and capabilities) in the security plan allows better mitigation and permits the most critical assets to be accorded priority based on the current network mission objectives.

We have outlined a straightforward, three-step MND process to transition IT-focused CND systems to mission-focused MND systems. The first step in making this an efficient and effective solution is to standardize and incorporate MND information into the CND log infrastructure. We propose that CEE be used as the basis for this standardization. Such expression and exchange of mission-relevant data is necessary to enable further options for creating adaptive MND systems and ensuring mission success. Additionally, CEE eliminates the underlying issues that would lead to reliance on third-party, proprietary solutions to interpret the volumes of mission and IT event data generated.