

Welcome and EMAP Program Overview

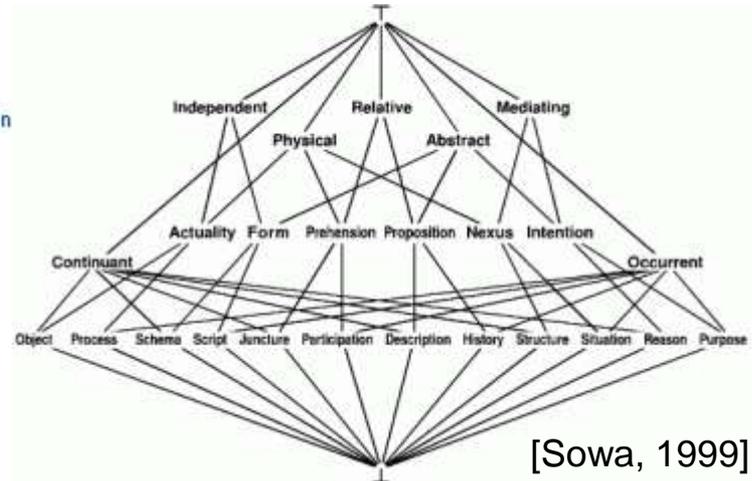


Paul Cichonski (NIST)
EMAP Lead





Introductions – Paul Cichonski



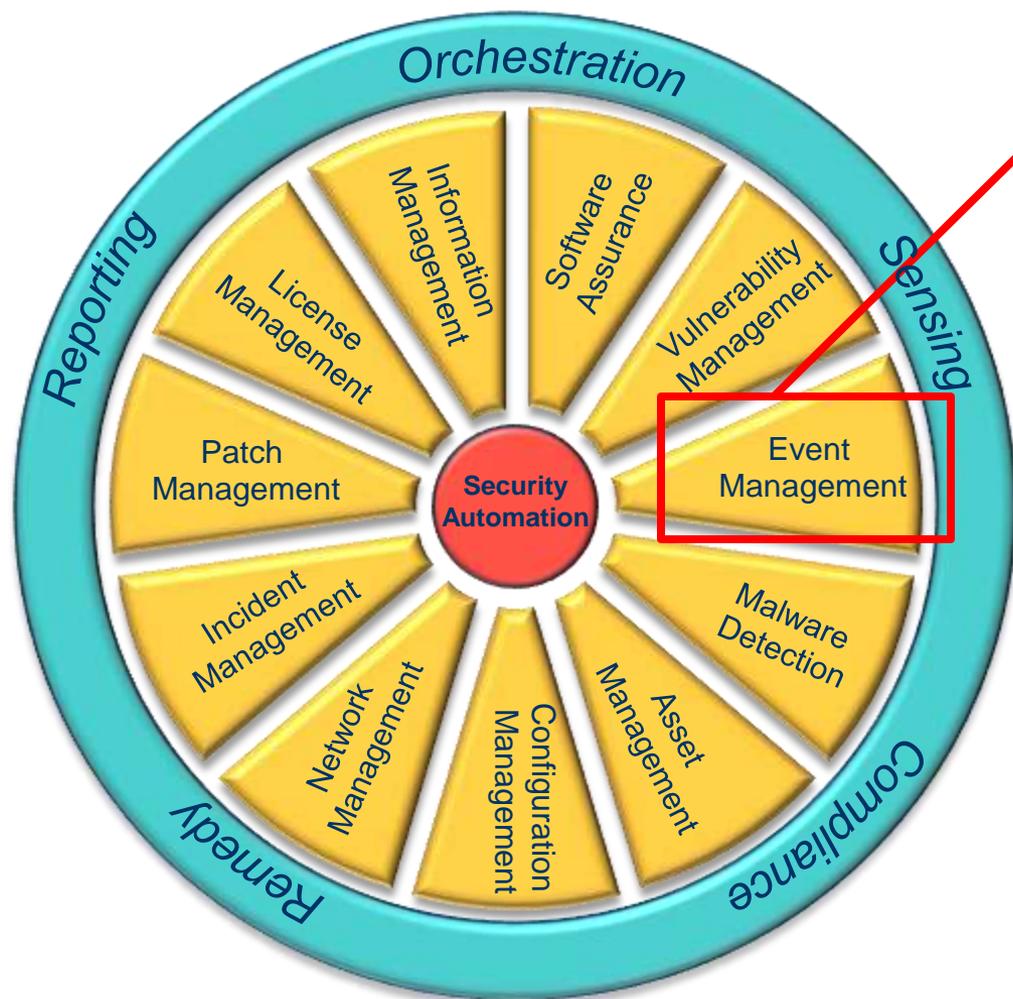


High Level Goals of the Event Management Automation Protocol (EMAP)

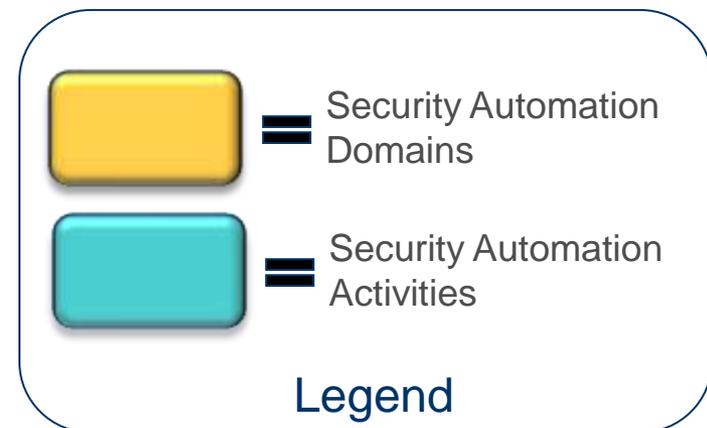
- Expand the effectiveness of the NIST Security Automation Program by establishing a suite of specifications standardizing the communication of digital event data.
 - EMAP will be a peer of the Security Content Automation Protocol (SCAP).
 - Relationships between the boundary objects in SCAP and EMAP domains will be captured.
- Develop and implement an EMAP Validation Program that will ensure compliance with EMAP specifications and increase the effectiveness of procurement decisions within organizations.



Context – Security Automation Program



- EMAP is attempting to standardize the machine communications within the Event Management domain.
- SCAP is focused on Configuration, Vulnerability and Asset Management.
- Other efforts are focused elsewhere → connections between efforts is critical.





Goal of Developer Days

- **Brief Ideas:** present initial ideas relating EMAP program and individual components, as well as the complexities related to standardizing machine communication within the IT event management domain.
- **Solicit Feedback and Requirements:** Developer Days is about discussion; we need to better understand the community's requirements in this area, and hear your feedback on our ideas.



NIST's Mission

“To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life.”

http://www.nist.gov/public_affairs/mission.cfm



EMAP Working Definitions (1 of 2)

- **Aggregation** — The identification and combination of two or more similar log entries. Aggregation is used to identify and remove duplicate log entries or to merge the details from log entries regarding the same event instance.
- **Correlation** — The association of two or more log entries of unique events. Correlation can be used to group events into a series, often by time sequence or causality.
- **Events** — Observable situations or modifications within an environment that occur over a time interval. An event may be a state change or reporting of an activity by a single component within a system, or may be an interaction between multiple systems. Events may occur at differing levels of abstraction and at multiple places along the log management path. As such, an event can describe an original (base) event, aggregated event, or correlated event.

As defined by the CEE Working Group (<http://cee.mitre.org/terminology.html>)



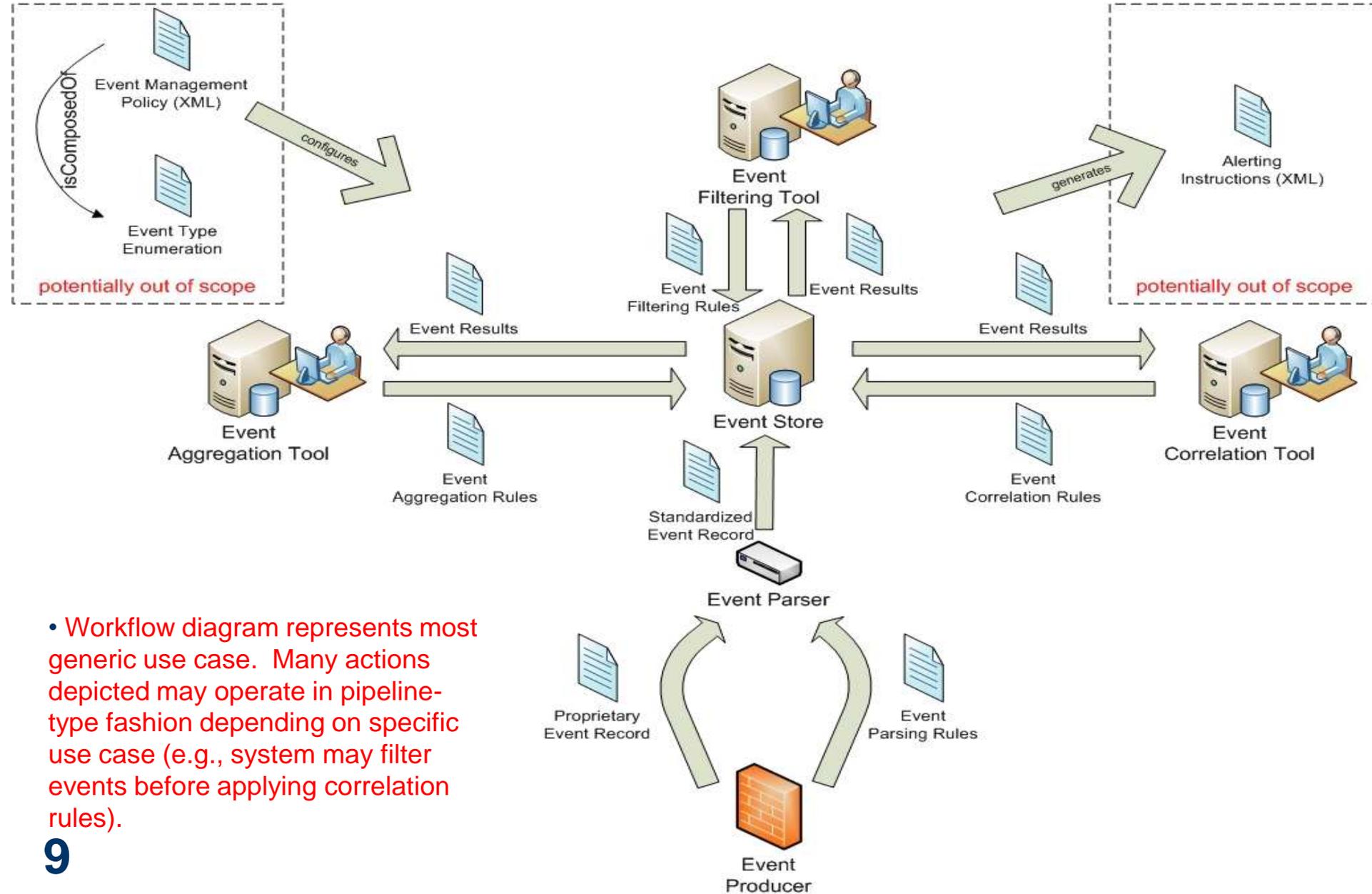
EMAP Working Definitions (2 of 2)

- **Event Record** — A collection of event fields that, together, describe a single event. Terms synonymous to event record include "audit record" and "log entry".
- **Log** — A collection of event records. Terms such as data log, activity log, audit log, audit trail, log file, and event log are often used to mean the same thing as log.

As defined by the CEE Working Group (<http://cee.mitre.org/terminology.html>)



EMAP Generic Architecture



- Workflow diagram represents most generic use case. Many actions depicted may operate in pipeline-type fashion depending on specific use case (e.g., system may filter events before applying correlation rules).



HIGH LEVEL USE CASES



High Level Use Cases (1 of 4)

- Incident Handling
 - Support the ability to identify ongoing incidents within an organization and the atomic events composing these incidents.
 - Support the ability to represent both atomic events and composite incidents in a machine readable way to allow automated sharing across partner organizations (i.e., enable distributed incident handling).
- Event Filtering
 - Support the ability to express event data information sharing policy in a machine readable way.
 - Support the ability to process machine-readable policy and automatically remove or anonymize event data before sharing with partner organization.



High Level Use Cases (2 of 4)

- Digital Forensics

- Support the ability to enable standardized signing of event data to provide chain of custody for auditors and digital forensic analysts.
- Support the ability to allow for intermediary systems to annotate event data without compromising the integrity of the original digital signature.

- Regulatory Compliance

- Support the ability to represent event management policy (e.g., PCI 10.2 & 10.3) in a machine-readable format.
- Support the ability to scan systems to ensure they are in compliance with policy.



High Level Use Cases (3 of 4)

- Real-Time Use of IT Event Data
 - Support the standardized exchange of IT event data between disparate components of an IT system.
 - Support the ability to build standardized publish/subscribe architectures for disseminating event data and alerts; to enable faster decision cycles in security tools.
- Standardization in Legacy Environments
 - Support the ability to interpret the proprietary log data from legacy IT tools through the lens of the EMAP standardized event vocabulary.
 - Support the ability to translate legacy log data in a decoupled manner that does not require large-scale updates to legacy code.



High Level Use Cases (4 of 4)

- Sharing of Rule Data
 - Support the ability of organizations to share standardized event correlation, filtering, and aggregation rule sets.
 - Support the ability to translate legacy rules, written in a non-standardized language, to a standardized rule exchange language; in a manner that protects proprietary content.



SOME DEFINITIONS TO HELP CREATE A SHARED UNDERSTANDING



Vocabulary and definitions for discussing our work

- **Scenario** – Composite, long-running activity occurring on a network.
- **Activity** – Specific phase of a scenario that is designed to complete some action to allow an analyst or system to identify, analyze, model, and report on the scenario occurring; all based on logs produced.
- **Data Flow** – A granular flow of data that occurs as a result of a particular activity within the context of a larger scenario.

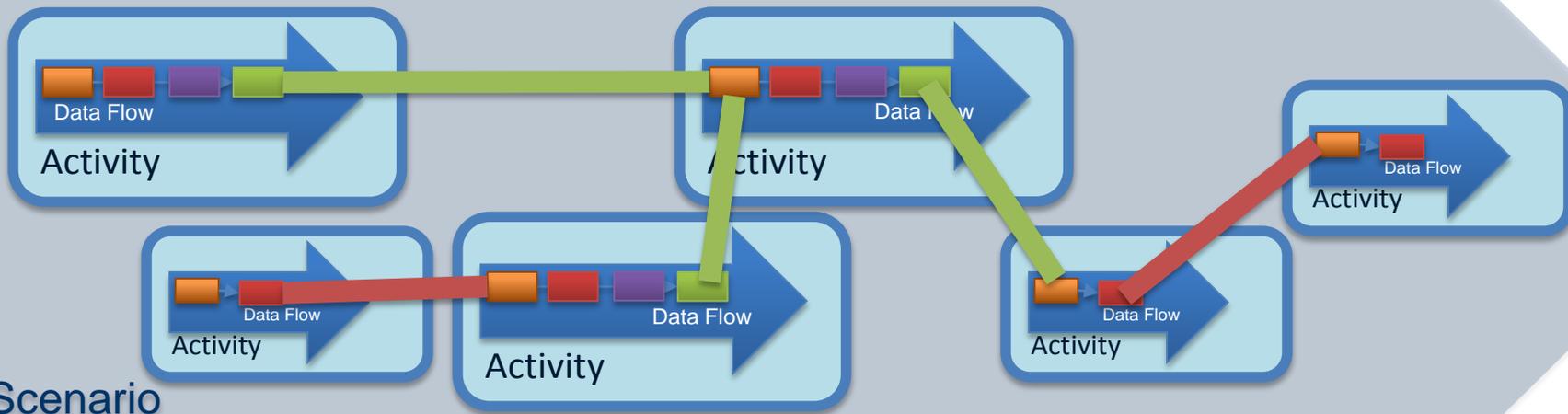
A scenario tells a story that has specific activities, all activities have data flows modeling how specific activity occurs within the context of the larger scenario taking place.

Purpose: These terms (and their relationships to each other) should provide context for discussing our work and will help us derive the appropriate requirements for EMAP.



A scenario tells a story that has specific activities, all activities have data flows

Some activities are disjoint, and will not appear together in the same scenario, but are different ways of instantiating the same scenario (i.e., scenarios may be instantiated in different ways depending on the capabilities of the organization).



Scenario



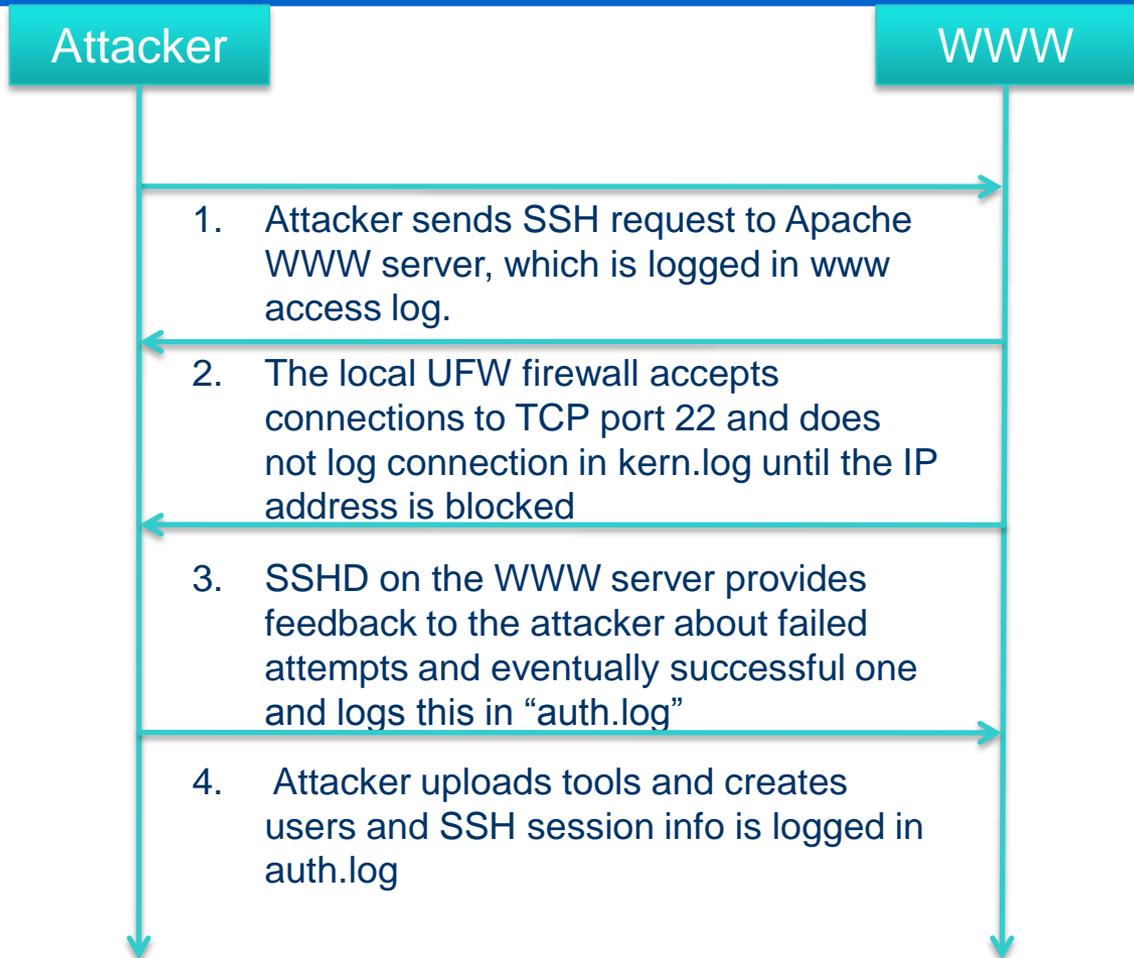
EMAP Activities

- Producing Standardized Event Record
- Producing Proprietary Event Record
- Parsing Logic Authoring
- Parsing Logic Execution
- Parsing Logic Migration and Sharing
- Event Consumption
- Rule Authoring
- Rule Execution
- Rule Migration and Sharing
- Alerting

* Note: not all activities are applicable to a specific scenario (depends on scope and complexity of scenario).



Example Scenario Involving a Malicious Incident



Log Source: honeynet challenge
(http://honeynet.org/challenges/2010_5_log_mysteries)



Activities instantiated through example scenario (simplified view)

Activity	Description	Data Flow
Producing Proprietary Event Record	As attacker's traffic interacts with www server, proprietary logs are produced.	Proprietary logs produced as a result of attacker's traffic.
Parsing Logic Authoring	Standardized log parsing instructions are created; describing how proprietary logs map to standardized model.	Parsing Logic author generates appropriate OEEL content for log types.
Parsing Logic Execution	Log parser executes standardized instructions to translate logs into standardized format.	Parsing instructions sent to parser, which executes them against legacy logs to produce standardized CEE logs.
Rule Authoring	Rule author creates correlation rule that models identified incident.	Rule author generates appropriate CERE rules.
Rule Execution	Correlation tool executes the standardized rules to identify other instances of this attack.	Rules sent to correlation tool, which executes them against an EMAP-compliant event store.



Similar [Event / Audit / Log] Management Standardization Efforts

- DMTF Cloud Auditing Data Federation Working Group
- Open Group X/Open Distributed Audit Service (XDAS) v2
 - David Corlette from Novell will be discussing this in more detail.



EXTRA



HIGH LEVEL USE CASES – MORE DETAIL



Use Case – Regulatory Compliance

- Event management regulations and policy (e.g., PCI 10.2 and 10.3) normally specifies the types of events, users, and systems to capture log data from. Policy also specifies frequency of logging, and retention time for log data. An event management team may use EMAP-expressed policy data to automatically configure their event management systems. Also, If the log data is EMAP compliant, then the auditor will be able to easily collect the data and verify compliance with policy using standardized queries.



Workflow for Regulatory Compliance Use Case

Step	Actor	Description	EMAP Component(s)
1	Policy Writer	Create high-level event management policy, written in natural language (NL).	N/A
2	Technical Policy Writer	Translate NL policy into machine readable format that captures: 1) Type of events to log 2) Types of systems to log 3) Types of users to log 4) Attributes of events to log 5) Frequency / retention of logging.	- Event Management Policy - Event Type Enumeration
3	Event Management Team	Ensure event producers produce correct type of event data, and that event data is stored according to policy. Ideally this process could be automated if EMAP compliant tools understand XML policy.	- All EMAP components



Use Case – Incident Handling

- Various agencies across the Federal Government are witnessing malicious activity across their respective networks. Along with government agencies, major companies in the private sector are also witnessing similar activity. Individuals from a few of companies publish initial *Event Correlation Rules*, for identifying the attack. As new information on the attack becomes available, other end users offer additional contributions and incremental improvements are made to the rules. Using vetted community input as a starting point, US-CERT develops and tests *Event Correlation Rules*, which it then shares within the Federal Government and private sector. Although institutions such as DoD, FDA, and USDA have implemented and support separate SIEM correlation technologies, each organizations' solution is EMAP compliant. Subsequently, each organization is able to utilize US-CERT's published rule set. While *Event Correlation Rules* provide a key component in the sharing of dynamic incident identification data, the Federal government must still implement standardized event detection capabilities across event management systems to achieve uniformity and coverage of its detective capabilities across EMAP compliant organizations.



Workflow for Incident Handling Use Case

Step	Actor	Description	EMAP Component(s)
1	Federal Agency	Agency identifies incident within internal networks. Agency then captures events associated with incident and reports data to US-CERT.	<ul style="list-style-type: none">- Event Producer- Standardized Event Record
2	US-CERT	US-CERT works with reporting agency, and other interested parties to model the incident and atomic events that comprise it. US-CERT then creates EMAP rules based on this model.	<ul style="list-style-type: none">- Standardized Event Record- Event Filtering Rules- Event Correlation Rules
3	US-CERT	US-CERT disseminates incident report containing EMAP rules.	<ul style="list-style-type: none">- Event Filtering Rules- Event Correlation Rules
4	Federal Agencies	All agencies within government scan EMAP compliant event stores to determine if incident is occurring on their networks.	<ul style="list-style-type: none">- Event Filtering Tool- Event Correlation Tool- Event Store- Event Results



Use Case – Event Filtering

- One government agency may wish to share information with another government agency. The agency adheres to government-wide digital access control policy that specifies that all event information may be shared, except the source and destination IP addresses. The digital access control policy provides EMAP-expressed machine readable filtering rules that the agency may use to scrub the sensitive information from the event data prior to sharing with the other organization. In addition to plain filtering rules, these rules may also contain obfuscation directives to replace real data with fake data.



Workflow for Event Filtering Use Case

Step	Actor	Description	EMAP Component(s)
1	Policy Writer	Create high-level digital access control policy relating to event data sharing between organizations.	N/A
2	Technical Policy Writer	Creates standardized event filtering rules that agencies may use to automate digital access control enforcement.	<ul style="list-style-type: none">- Event Management Policy- Event Filtering Rules
3	Event Management Team	Ensure event stores only provide external access through channels that enforce digital access control policy using standards-based filtering rules that will work on any EMAP-compliant vendor solution.	<ul style="list-style-type: none">- Event Store- Event Filtering Rules- Event Filtering Tool- Event Results



Use Case – Digital Forensics

- During legal disputes, forensic examiners will often rely on digital event records as a source of evidence to prove/disprove their claims. However, digital event logs must adhere to certain standards relating to log integrity and chain of custody for logs to be admissible in a court of law. If an *Event Producer* is required to comply with these standards, they may need to ensure that log data is digitally signed, and that the digital signature can be traced back to a reliable source (e.g., a Trusted Platform Module). Also, any intermediary systems wishing to augment log data (e.g., to add tagging metadata) must do so in a way that does not break the chain of custody. This means that intermediary systems must ensure that modifications to log records do not invalidate original digital signatures. A *Standardized Event Record* specification must provide mechanisms for maintaining log integrity and chain of custody. Leveraging this standardized mechanism, forensic examiners may use the same method for proving log integrity across a wide variety of EMAP compliant event logs.



Workflow for Digital Forensics Use Case

Step	Actor	Description	EMAP Component(s)
1	Event Producer	Event Producer produces event logs and applies digital signatures to log records. This digital signature may be applied at either individual event record level, or at collection level, depending on processing/integrity requirements.	<ul style="list-style-type: none">- Event Producer- Standardized Event Record
2	Event Parser	If the Event Producer produced log data adhering to a proprietary log format, an event parser must transform the logs into a standardized format in a way that does not invalidate the original digital signature.	<ul style="list-style-type: none">- Event Parser- Event Parsing Rules
3	Intermediary System	Intermediary system processes log data from event producer before it is accepted into Event Store. The Intermediary system appends tagging metadata to log records, while maintaining chain of custody. Log data is then passed to Event Store.	<ul style="list-style-type: none">- Standardized Event Record- Event Store <p>(note: concept of intermediary system not currently captured in generic workflow diagram)</p>
4	Forensic Examiner	Forensic examiner queries Event Store for incident-specific activity. All Event Results adhere to legal standards for admissibility in court.	<ul style="list-style-type: none">- Event Store- Event Filtering Rules- Event Filtering Tool- Event Correlation Rules- Event Correlation Tool- Event Results



Use Case – EMAP Adoption in Legacy Environments

- The success of event management automation is largely dependent on the ease of adoption within an organization. Organizations that adopt EMAP will likely have a variety of legacy *Event Producers* that will generate log data according to a proprietary syntax and not support the EMAP *Standardized Event Record* syntax. In these cases, the organization may create *Event Parsing Rules* that will run in an EMAP compliant *Event Parser*. These *Event Parsing Rules* will instruct the parser on how to translate *Proprietary Event Data* into the *Standardized Event Record* syntax. Through this modular approach organizations may begin to leverage EMAP without the need to update all legacy software within their network. In addition, since these rules will run in any EMAP compliant *Event Parser*, organizations may share these rules with partner organizations, or upload them to public repositories promoting community collaboration.



Workflow for EMAP Adoption in Legacy Environments Use Case

Step	Actor	Description	EMAP Component(s)
1	Event Management Analyst	Analyst identifies software within the network that does not produce EMAP compliant Standardized Event Data. Analyst then writes EMAP Event Parsing Rules instructing an Event Parser on how to translate proprietary event data syntax to standardized syntax (e.g., Apache WWW format to CEE format).	- Event Producer - Event Parsing Rules
2	Event Management Analyst	Analyst then configures the Event Parser to use the specific translation rules when processing event data from specific Event Producers (e.g., in this case all Apache WWW servers).	- Event Producer - Event Parsing Rules - Event Parser
3	Event Parser	Event parser translates all proprietary event record data from proprietary syntax to standardized syntax. Parser then passes standardized event record data to Event store for additional processing.	- Event Parsing Rules - Event Parser - Standardized Event Record - Event Store
4	Organization	Organization uploads new standardized Event Parsing Rules to public repository promoting open collaboration.	- Event Parsing Rules



Use Case – Real Time Event Management

- The majority of the use cases presented focus on log and audit management, in these scenarios the actors normally wait until logs have been processed, aggregated and filtered before running correlation rules. An alternative scenario for event data is sometimes referred to as near real-time event management. This use case involves a more cohesive ecosystem view where communication occurs rapidly between disparate *Event Producers*. This type of use case may utilize a publish/subscribe architecture with a faster decision cycle for detecting attacks and taking corrective action.

For example, consider the scenario where a Network Intrusion Detection System (NIDS) identifies a potential intrusion occurring on a specific network segment. The NIDS publishes the *Standardized Event Records* describing this intrusion to an enterprise service bus for dissemination to interested parties. A firewall responsible for the network segment under investigation has previously registered with the enterprise service bus (ESB) to receive all messages related to the IP range for its network segment. The firewall used terms defined within the *Standardized Event Record* data model to complete this registration. The ESB then delivers the intrusion alert to the firewall, which is able to terminate the suspicious connection.



Workflow for Real Time Event Management Use Case

Step	Actor	Description	EMAP Component(s)
1	Vendor X Firewall	Firewall creates filtering/correlation rules that identify events pertaining to its area of responsibility. Firewall then uses standardized connection protocols to subscribe to an enterprise service bus (ESB) messaging system. The firewall uses the rules as the method for asserting what messages are applicable.	<ul style="list-style-type: none">- Standardized Event Record- Event Filtering Rules- Event Correlation Rules- Standardized Connection Protocols for pub/sub architecture (not currently an EMAP component)
2	Vendor Y Network Intrusion Detection System (NIDS)	NIDS identifies potential intrusion on network segment, generates event data representing this intrusion and publishes it to the ESB using a standardized connection protocol.	<ul style="list-style-type: none">- Event Producer- Standardized Event Record- Standardized Connection Protocols for pub/sub architecture (not currently an EMAP component)
3	ESB	ESB compares events from IDS to set of existing notification assertions. ESB determines events match Vendor X Firewall's notification rules and delivers events to the firewall.	<ul style="list-style-type: none">- Standardized Event Record- Event Filtering Rules- Event Correlation Rules- Standardized Connection Protocols for pub/sub architecture (not currently an EMAP component)
4	Firewall	Analyzes events, identifies suspicious connection(s) and terminates them.	<ul style="list-style-type: none">- Standardized Event Record



Use Case – Sharing Rule Data

An organization has created a large knowledge repository of proprietary event management correlation rules. The organization may wish to translate these rules to the EMAP compliant *Event Correlation Rule* format to share with partner organizations, or customers. However, the organization must ensure that proprietary data contained within the rules is not translated into the standardized format. To accomplish this task, the organization may use a *Rule Translation Language* to express the translation logic; this translation logic will capture the steps for performing the mapping between logical components in the two rule language as well as the instructions on how to handle proprietary data. An EMAP compliant tool could process the translation logic to perform automatic translation on the organization's rule data.