Event Management Automation Protocol (EMAP)

Update

George Saylor

NIST

(U) Agenda

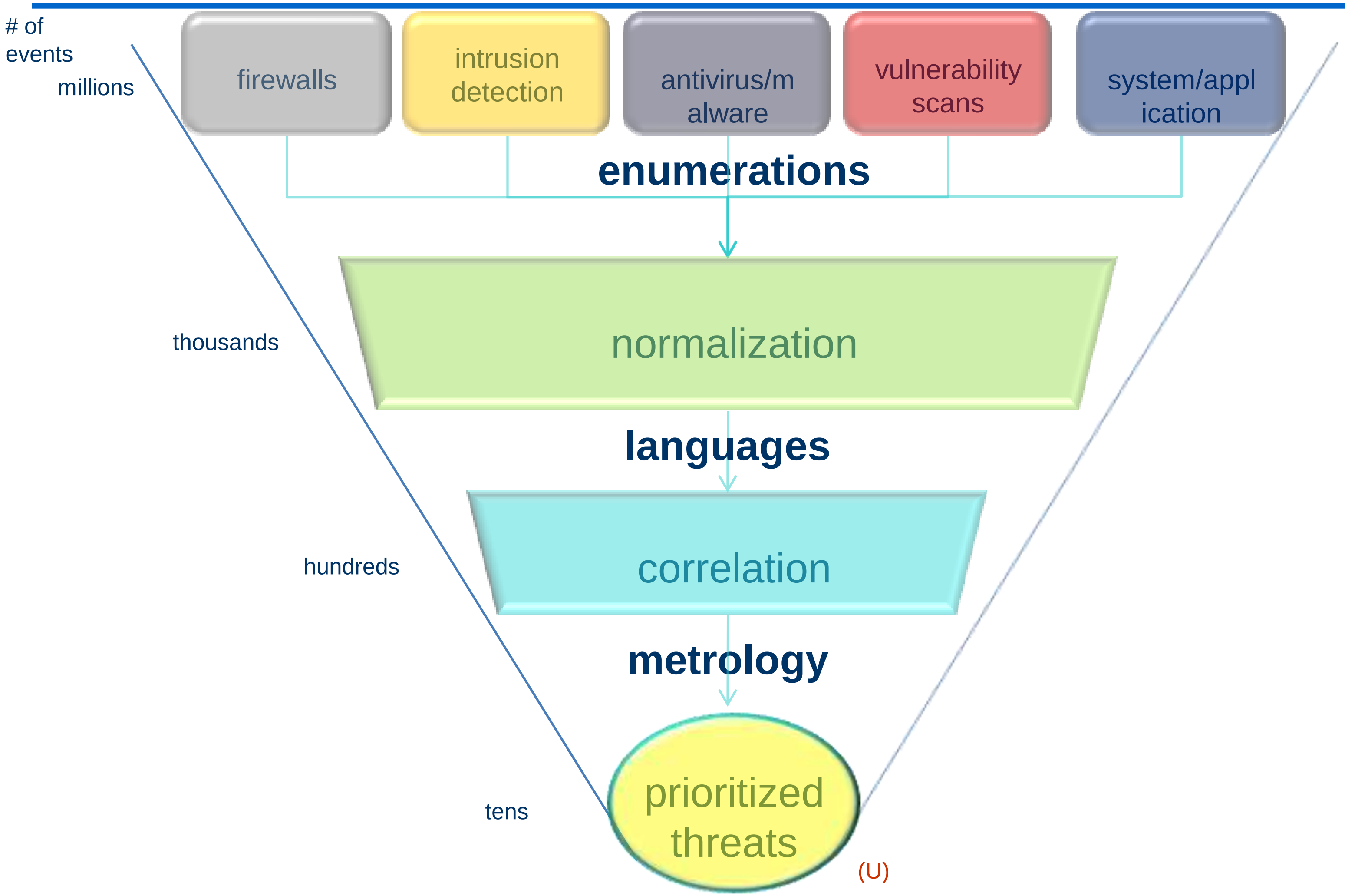
- (U) What is the problem?
- (U) What is EMAP?
- (U) How will EMAP work?
- (U) Notional EMAP components
- (U) The bigger picture

(U) The Problem

- (U) “Tower of Babel”
  - Too many log formats
  - Limited past success in developing log standards
- (U) Resources being spent on mundane “security hygiene” tasks
  - Parsing and consolidating logs
  - Event collection, correlation, categorization

(U) Event Funnel

(U)



(U) What is EMAP?

(U)

Languages

Express logs and policies

- Log formats
- Log correlation rules
- Logging configuration
- Audit Settings
- Normalization

Metrics

Event scoring framework

- Severity of logged events
- Alert level

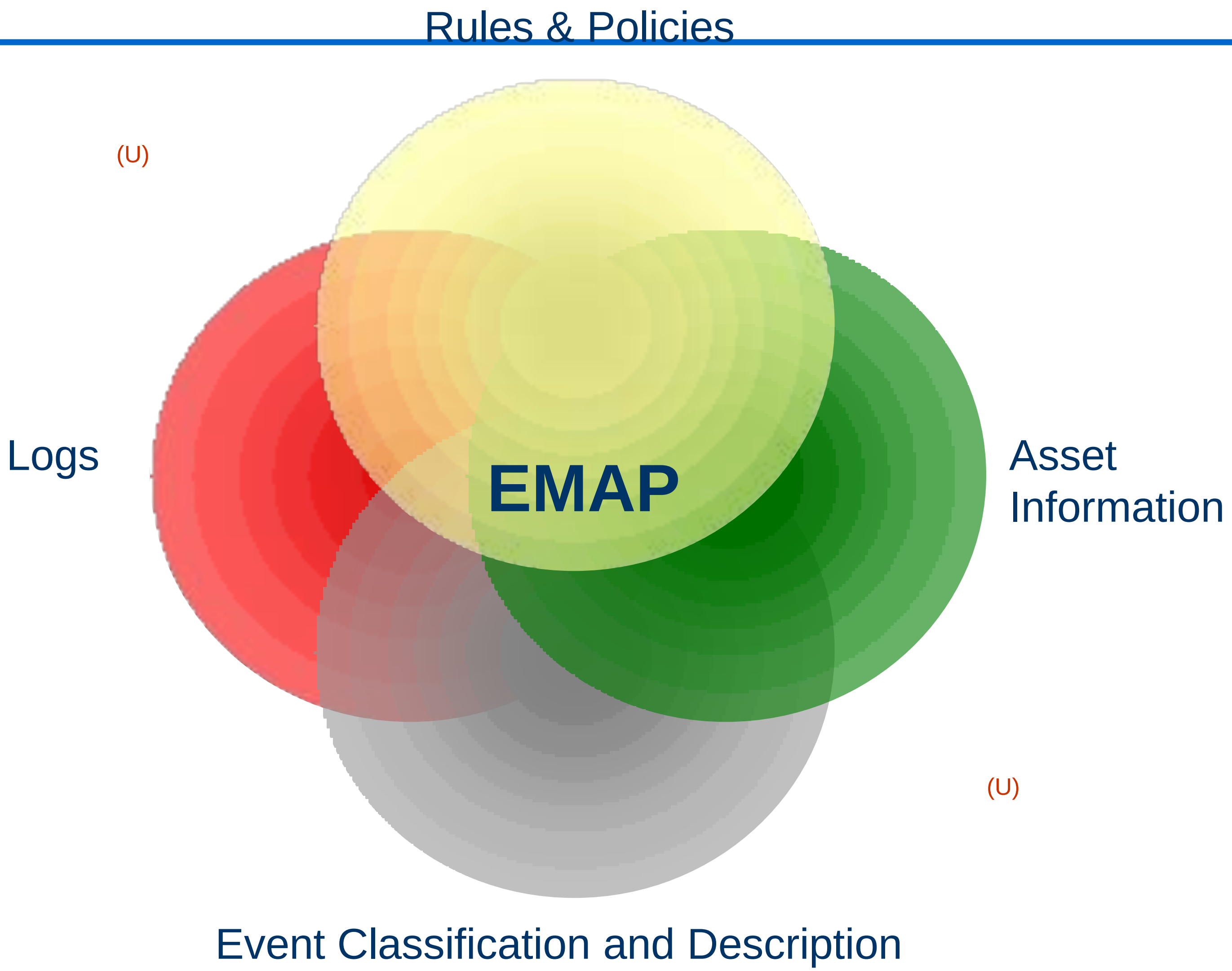
Enumerations

Convention for identifying and naming

- Log taxonomy
- Enrichment information
- Observables

(U)

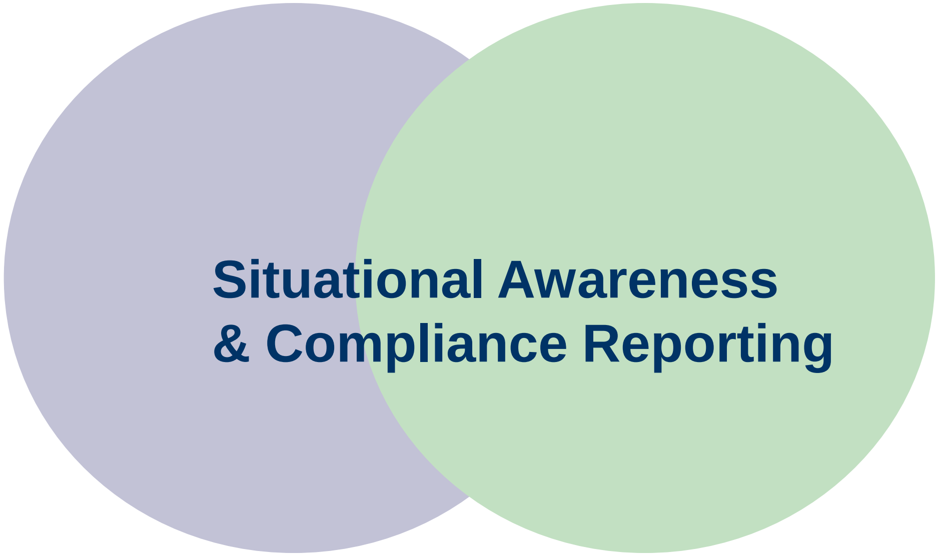
(U) Network Monitoring, Logging, and Audit Through EMAP



(U) Fusion

(U)

SCAP

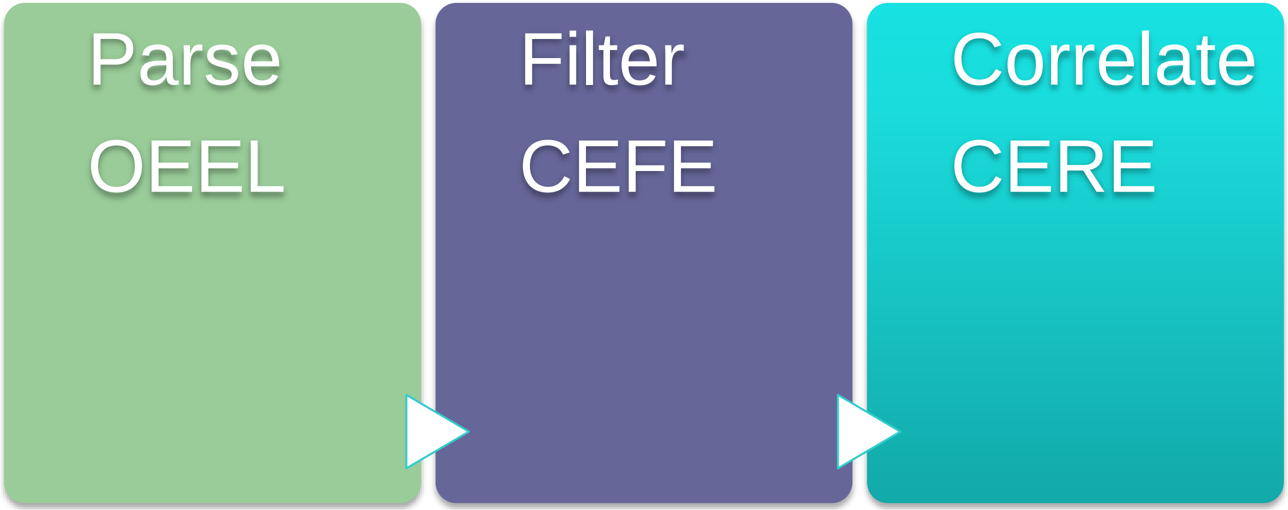


EMAP

(U)

(U) How it all works

(U)



Parse

OEEL

Filter

CEFE

Correlate

CERE

(U)

Feasibility Study

- Feasibility Study completed in 2009

✓ Determined that a limited scope protocol is possible

✓ Identified existing work that would support the effort

✓ Identified specifications requiring development

✓ Began authoring EMAP whitepaper

EMAP White Paper

- A white paper describing the EMAP concept and notional architecture is in draft

✓ Use cases

✓ Proposed specifications

✓ Proposed interactions between specifications

✓ Currently in draft – under review

(U) Open Event Expression Language (OEEL)

- (U) A language to express parsing logic external to an application
  - Allows parsers to be created without changing compiled code
  - Can go from any format to any format as long as both format and transformation rules can be expressed
- (U) Aimed at lessening (not eliminating) parsing of log sources.
- (U) A limited proof-of-concept completed

Open Event Expression Language

- A new specification is proposed to externalize parsing logic into a
- standard syntax

✓ Standardized expression of parsing logic

✓ Reduces burden of adding new log sources

✓ Language proposal in draft

✓ Language samples under review

✓ Limited prototype

(U) Common Event Filter Expression (CEFE)

- (U) Conceptually an expression of rules to filter out unwanted log entries (reduction)
- (U) Currently in research
  - Currently the Rule Interchange Format (W3C) is being considered
  - Will likely have a common base with CERE
  - Notionally a data exchange standard rather than an executable language (unless a vendor supports RIF)

(U) Common Event Rule Expression (CERE)

- (U) Conceptually an expression of rules to search and correlate log entries (correlation)
- (U) Currently in research
  - Currently the Rule Interchange Format (W3C) is being considered
  - Heavily researching the expressability of correlation rules in RIF
  - Notionally a data exchange standard rather than an executable language (unless a vendor supports RIF)

Common Event Rules

- A new specification is being investigated to express rules for
- pattern matching and expression of correlation rules

✓ Common syntax to express pattern match for alerting

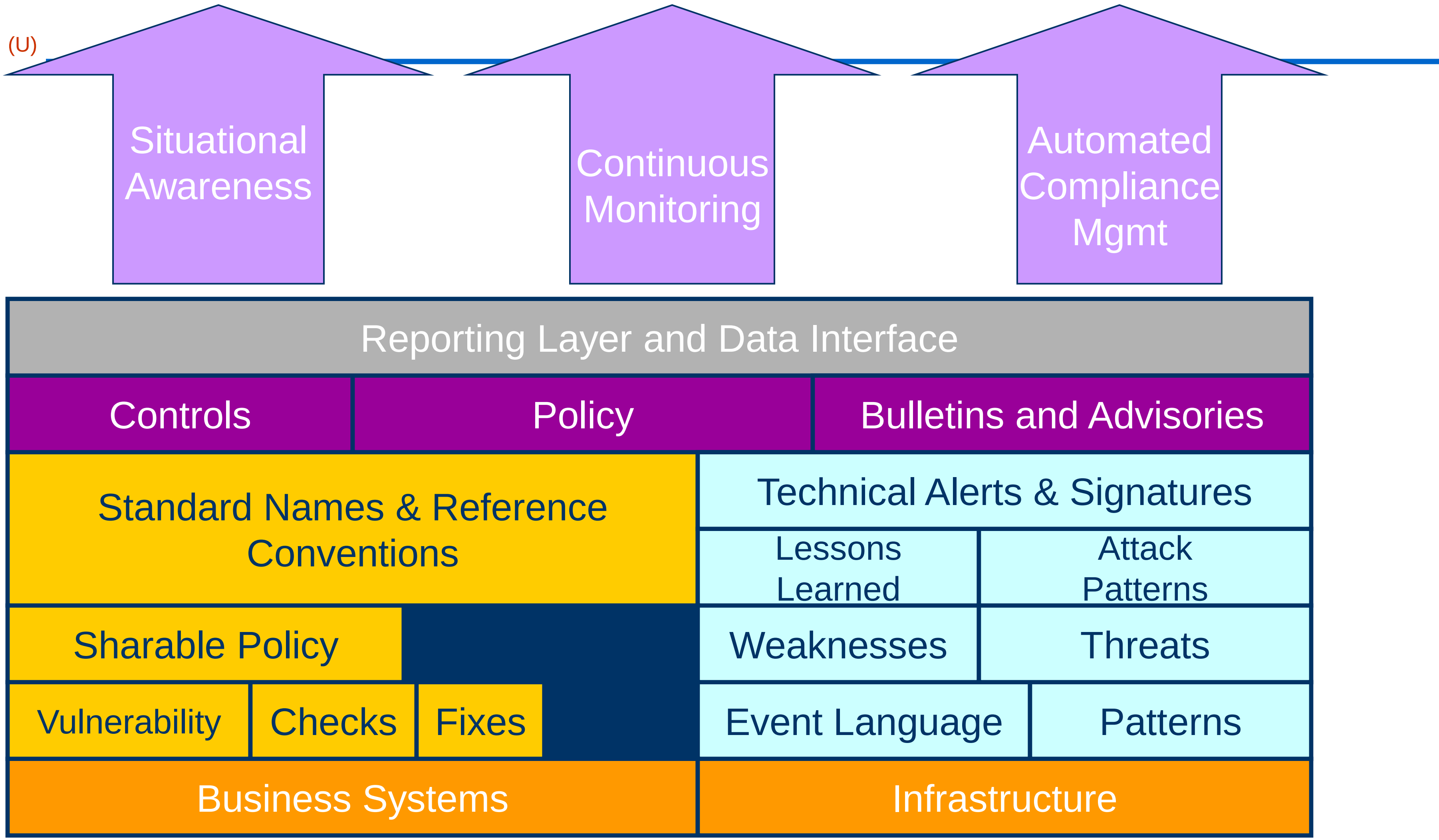
✓ Express correlation logic in a standardized format

✓ Analyzing technologies such as RIF, RuleML, Drools, as well as current SIEM technology

✓ Language outline in draft

(U) Notional Security Data Model

(U)



Situational Awareness

Continuous Monitoring

Automated Compliance Mgmt

Reporting Layer and Data Interface

Controls | Policy | Bulletins and Advisories

Standard Names & Reference Conventions

Technical Alerts & Signatures

Lessons Learned | Attack Patterns

Sharable Policy

Weaknesses | Threats

Vulnerability | Checks | Fixes

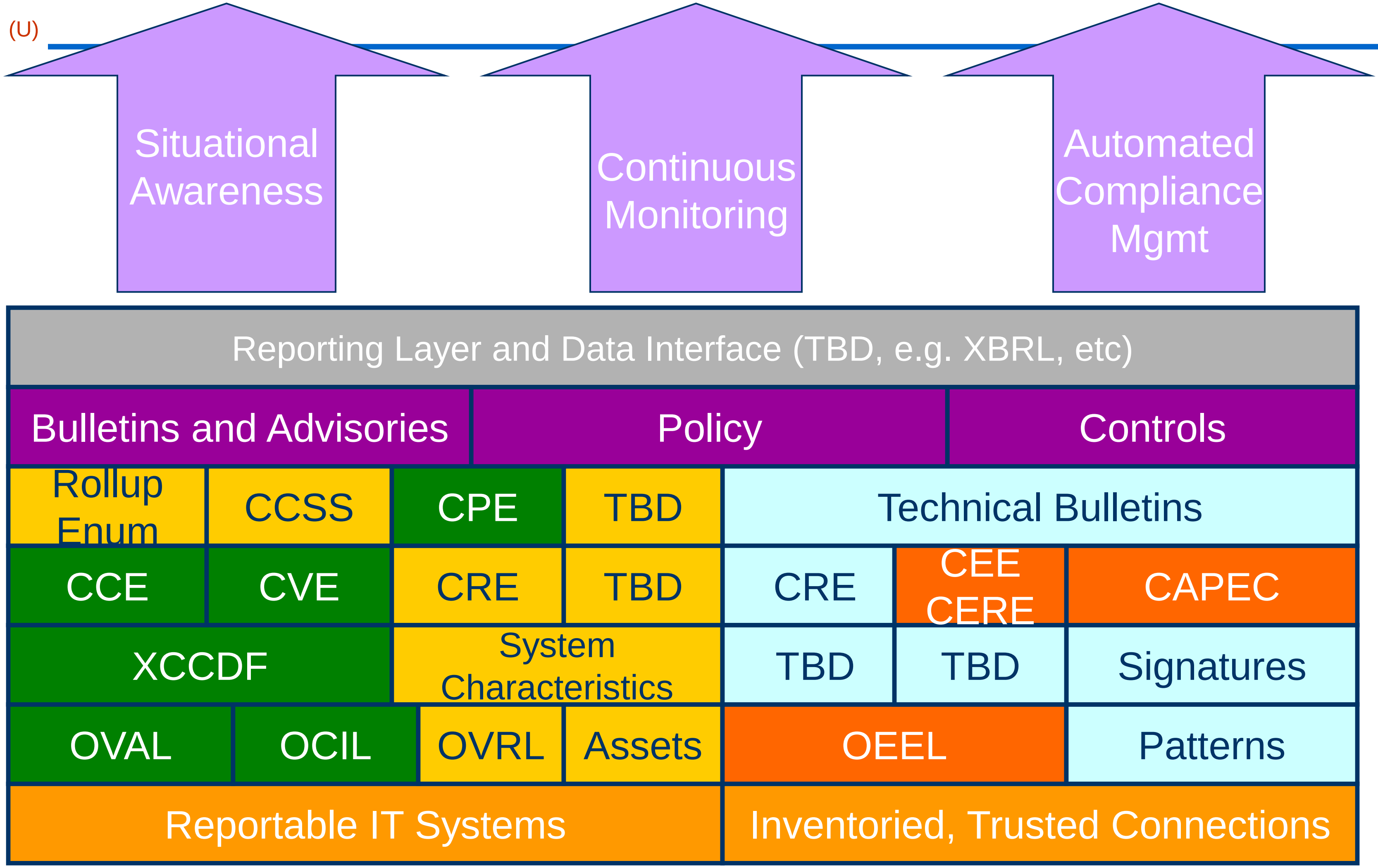
Event Language | Patterns

Business Systems | Infrastructure

(U)

(U) Notional Specifications-Based Security Automation

(U)



Situational Awareness

Continuous Monitoring

Automated Compliance Mgmt

Reporting Layer and Data Interface (TBD, e.g. XBRL, etc)

Bulletins and Advisories | Policy | Controls

Rollup Enum | CCSS | CPE | TBD | Technical Bulletins

CCE | CVE | CRE | TBD | CRE | CEE CERE | CAPEC

XCCDF | System Characteristics | TBD | TBD | Signatures

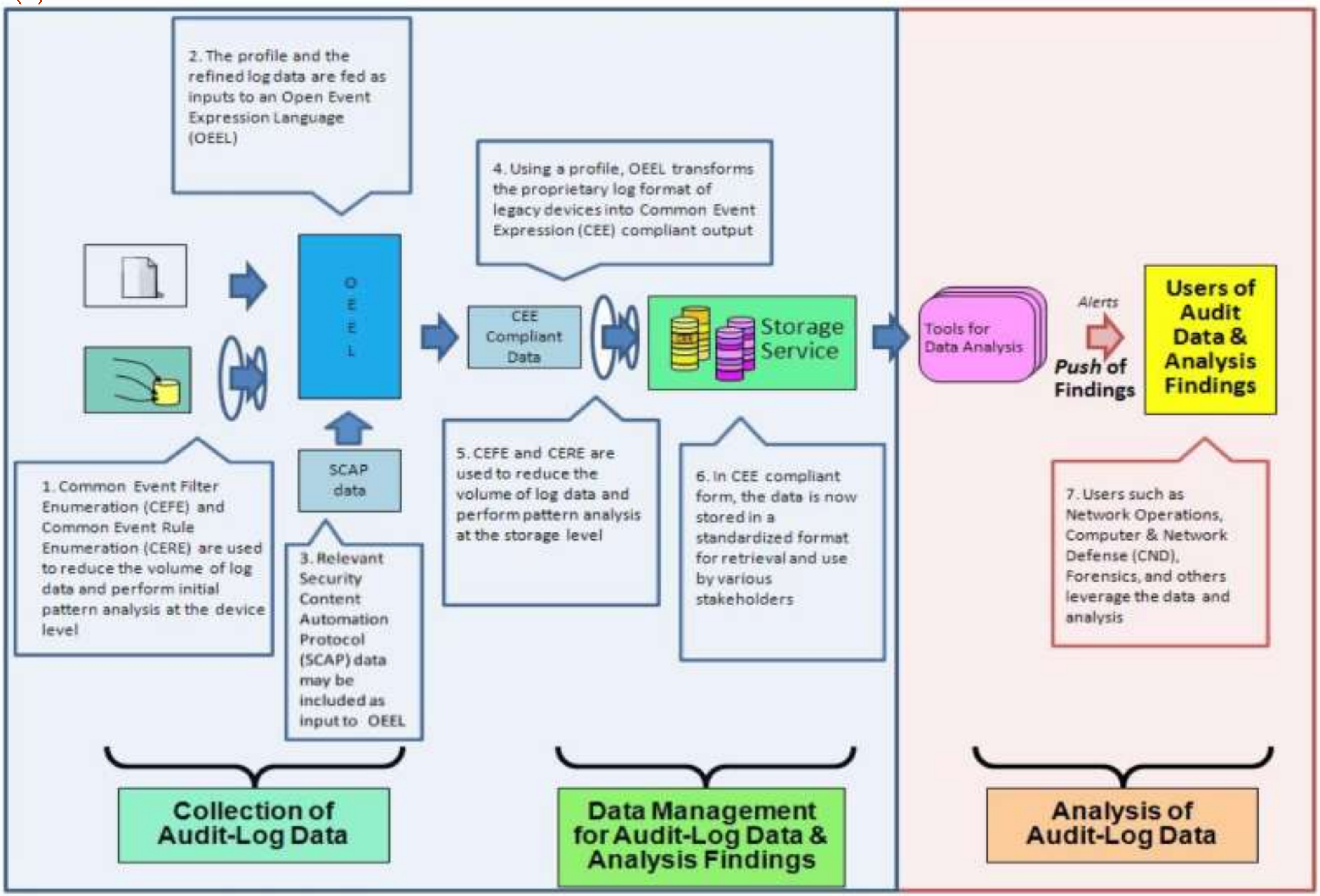
OVAL | OCIL | OVRL | Assets | OEEL | Patterns

Reportable IT Systems | Inventoried, Trusted Connections

(U)

(U) Basic EMAP Components (notional)

(U)



O E E L
CEE Compliant Data
SCAP data
Storage Service
Tools for Data Analysis
Alerts
Push of Findings
Users of Audit Data & Analysis Findings
Collection of Audit-Log Data
Data Management for Audit-Log Data & Analysis Findings
Analysis of Audit-Log Data

1. Common Event Filter Enumeration (CEFE) and Common Event Rule Enumeration (CERE) are used to reduce the volume of log data and perform initial pattern analysis at the device level

2. The profile and the refined log data are fed as inputs to an Open Event Expression Language (OEEL)

3. Relevant Security Content Automation Protocol (SCAP) data may be included as input to OEEL

4. Using a profile, OEEL transforms the proprietary log format of legacy devices into Common Event Expression (CEE) compliant output

5. CEFE and CERE are used to reduce the volume of log data and perform pattern analysis at the storage level

6. In CEE compliant form, the data is now stored in a standardized format for retrieval and use by various stakeholders

7. Users such as Network Operations, Computer & Network Defense (CND), Forensics, and others leverage the data and analysis

(U)

Questions / Comments?

George Saylor
george.saylor@nist.gov