



# Common Event Record Version 0.5 for Pilot

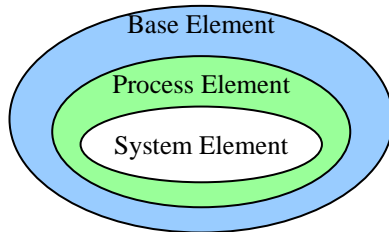
# Pilot Common Event Record Design

- Must represent four types of events
  - Application – events that occur within an application
  - Network – occur within a network (flow based)
  - Security – changes or differences in security policy (from IDS or firewalls)
  - System – OS and hardware related events
- Provide a common structure to enable correlation of events (base element)
- Leverage existing data manipulation tools by representing data within an XML framework

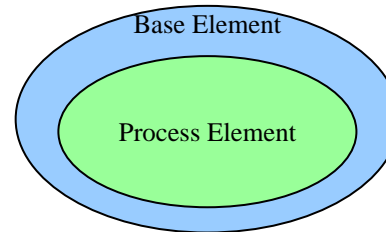
# XML Schema Nesting

- ccBay events are constructed as nested XML sub-schemas:
  - System Event
    - A System element inside a Process element inside an Base element.
  - Application Event
    - A Process element inside an Base element.
  - Security Event
    - A Security element inside a Network element inside an Base element.
  - Network Event
    - A Network element inside an Base element.

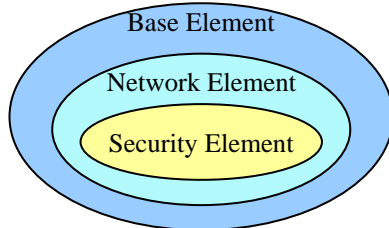
# XML Schema Nesting (continued)



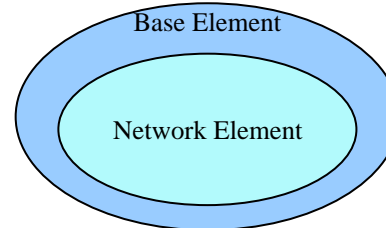
System Event



Application Event



Security Event



Network Event

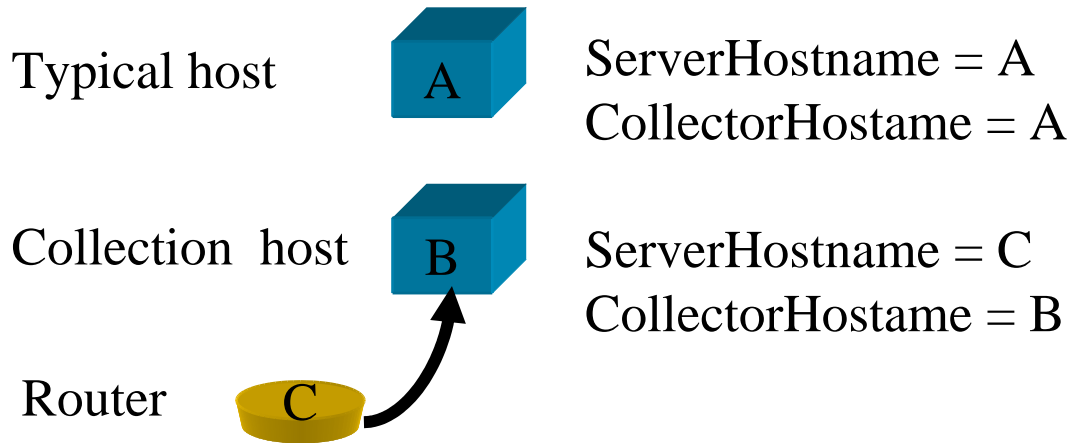
Illustration of nested XML elements.

# BaseElement XML Schema

```
<org.Internet2.Middleware.ccBay.BaseElement Version = "0.1">
  <Record>
    <Tag STRING/> <!--Optional -->
    <TimeStart TIMESTAMP/> <!-- Required -->
    <TimeEnd TIMESTAMP/> <!-- Optional -->
    <ServerHostname FQDN/> <!-- Optional -->
    <ServerIP IP_ADDRESS/> <!-- Required -->
    <CollectorHostname FQDN/> <!-- Optional -->
    <CollectorIP IP_ADDRESS/> <!-- Required -->
    <CollectorName STRING/> <!-- Required -->
    <CollectorVersion FLOAT/> <!-- Required -->
    <WarnLevel STRING/> <!-- Required -->
    <EventMessage STRING/> <!-- Required -->
    <org.Internet2.Middleware.ccBay.ProcessElement/> <!-- Optional -->
    <org.Internet2.Middleware.ccBay.NetworkElement/> <!-- Optional -->
  </Record>
</org.Internet2.Middleware.ccBay.BaseElement>
```

# BaseElement – Observation Points

- ccBay events can be observed directly or indirectly
  - ServerHostname – the system that ccBay resides on
  - CollectorHostname – the system that produces the events



# *BaseElement* – Warning Levels

- EMERG - system is unusable
- ALERT - action must be taken immediately
- CRIT - critical conditions
- ERR - error conditions
- WARNING - warning conditions pre-error
- NOTICE - normal but significant condition
- INFO - informational
- DEBUG - debug-level events

# BaseElement – User Tags

- Meaning can be given to an event by writing a normalizer that inserts a user defined tag based on an event criteria
  - Specific data that enhances the event
    - UserTag = “SwapUsed:1.67GB”
    - UserTag = “cd@cmu.edu changed config”
    - UserTag = “<throughput>993</throughput>”
  - Anonymized user hashes for tracking and debugging
    - UserTag = “user:d3b07384d113edec49eaa6238ad5ff00”

# ProcessElement XML Schema

```
<org.Internet2.Middleware.ccBay.ProcessElement Version = "0.1">  
  <Record>  
    <ProcessID INT/> <!-- Required -->  
    <ProcessName STRING/> <!-- Required -->  
    <ProcessOwner STRING/> <!-- Required -->  
    <org.Internet2.Middleware.ccBay.SystemEvent/> <!-- Optional -->  
  </Record>  
</org.Internet2.Middleware.ccBay.ProcessElement>
```

# SystemEvent XML Schema

```
<org.Internet2.Middleware.ccBay.SystemEvent Version = "0.1">  
  <Record>  
    <Facility STRING/> <!-- Optional -->  
    <Subsystem STRING/> <!-- Optional -->  
  </Record>  
</org.Internet2.Middleware.ccBay.SystemEvent>
```

```
<org.Internet2.Middleware.ccBay.NetworkElement Version = "0.1">
  <Record>
    <SourceIP IP_ADDRESS/> <!-- Required -->
    <DestinationIP IP_ADDRESS/> <!-- Required -->
    <NextHopIP IP_ADDRESS/> <!-- Required -->
    <InterfaceIn STRING/> <!-- Required -->
    <InterfaceOut STRING/> <!-- Required -->
    <Packets INT/> <!-- Required -->
    <Octets INT/> <!-- Required -->
    <SourcePort INT/> <!-- Required -->
    <DestinationPort INT/> <!-- Required -->
    <IPTypeOfService STRING/> <!-- Required -->
    <Protocol STRING/> <!-- Required -->
    <TypeOfService STRING/> <!-- Required -->
    <SourceAutonomousSystem STRING/> <!-- Required -->
    <DestinationAutonomousSystem STRING/> <!-- Required -->
    <SourceMask OCTAL/> <!-- Required -->
    <DestinationMask OCTAL/> <!-- Required -->
    <org.Internet2.Middleware.ccBay.SecurityEvent/> <!-- Optional -->
  </Record>
</org.Internet2.Middleware.ccBay.NetworkElement>
```

# SecurityElement XML Schema

```
<org.Internet2.Middleware.ccBay.SecurityElement Version = "0.1">  
  <Record>  
    <ReferenceSystem STRING/> <!-- Required -->  
    <TCPHeader INT/> <!-- Optional -->  
    <UDPHeader INT/> <!-- Optional -->  
    <ICMPHeader INT/> <!-- Optional -->  
    <RawData STRING/> <!-- Optional -->  
  </Record>  
</org.Internet2.Middleware.ccBay.SecurityElement>
```

# System Event Normalization Example

- Raw entry from /var/log/messages:

Jul 29 15:07:27 cmu1 sshd[11157]: Failed password for illegal user Administrator from ::ffff:192.168.2.6 port 4324 ssh2

- Raw entry normalized as XML as a System Event:

```
<org.Internet2.Middleware.ccBay.BaseElement Version="0.1">
  <Record>
    <TimeStart>Jul 29 15:07:27</TimeStart>
    <ServerHostname>cmu1</ServerHostname>
    <ServerIP>192.168.2.2</ServerIP>
    <CollectorHostname>cmu1</CollectorHostname>
    <CollectorIP>192.168.2.2</CollectorIP>
    <CollectorName>ccbay-slogd</CollectorName>
    <CollectorVersion>0.1</CollectorVersion>
    <WarnLevel>info</WarnLevel>
    <EventMessage>Failed password for illegal user Administrator from ::ffff:192.168.2.6 port 4324 ssh2</EventMessage>
  </org.Internet2.Middleware.ccBay.ProcessElement>
  <Record>
    <ProcessName>sshd</ProcessName>
    <ProcessID>11157</ProcessID>
    <org.Internet2.Middleware.ccBay.SystemElement>
      <Record>
        <Facility>User</Facility>
      </Record>
    </org.Internet2.Middleware.ccBay.SystemElement>
  </Record>
</org.Internet2.Middleware.ccBay.ProcessElement>
</Record>
</org.Internet2.Middleware.ccBay.BaseElement>
```