The Case for Comprehensive Diagnostics

CyDAT - Cyber-center for Diagnostics, Analytics and Telemetry

Chas DiFatta (chas@cmu.edu)
Dan Klein (dvk@lonewolf.com)
Mark Poepping (poepping@cmu.edu)

Carnegie Mellon

Diagnostics…?

You discover your car has a flat tire...

- You fix it you move on

It’s flat again a week later...

- Valve problem?
- Nails in the driveway?
- Neighbor kid?

Can you check all failure possibilities?

- Might help if you knew when air started leaking

Cars… Computers…

You discover your Sendmail daemon crashed...

- You restart it and you move on

It crashes again a day later...

- Configuration problem?
- Performance or resource problem?
- New bug or integration problem with spam engines?
- Security vulnerability? Is it really “my” sendmail running or a rogue daemon?

Why Diagnostics?

- Things break, in complicated, partial ways – and it matters
- Systems built to ‘get it working’, not to be ‘fixed’
  - Meter/maintain/fix after installation?
  - The maintainer learns how… but it’s a struggle
- Software reuse and layered infrastructures create dynamic dependencies
  - Diagnostic data may not be available at all
  - Certainly doesn’t follow service path
  - Minimally ‘out of band’, often ‘out of question’
- Service Plane + Management Plane + *Diagnostic Plane*

Who are the Diagnosticians?

In IT (lots of other diagnostic domains):

- Applications Support Personnel
- Systems Administrators
- Network Support Staff
- Security Response Folks
- Managers of Computing Infrastructure
- Help Desk
- Ordinary Users

Who are the Diagnosticians?

In IT (lots of other diagnostic domains):

- Applications Support Personnel
- Systems Administrators
- Network Support Staff
- Security Response Folks
- Managers of Computing Infrastructure
- Help Desk
- Ordinary Users

Everybody

Banes of Diagnosticians

Validated through Interviews

- Limited access to slices of diagnostic data
- Discovering valuable information in a sea of data
- Correlating different diagnostic data types
- Providing evidence for non-repudiation of a diagnosis
- Finding time to create tools to transfer diagnostic knowledge to less skilled organizations and/or individuals (automation)

An Illustration

Someone reports the payroll application seemed slow at 2pm

- You look around, but it seems fine and you move on.

Someone else reports the problem again a week later...

- Configuration or firmware problem?
- Downstream congestion problem caused by large file transfers?
- Networking problem?
- How many potential failure scenarios?

An Illustration (2)

What's Involved?

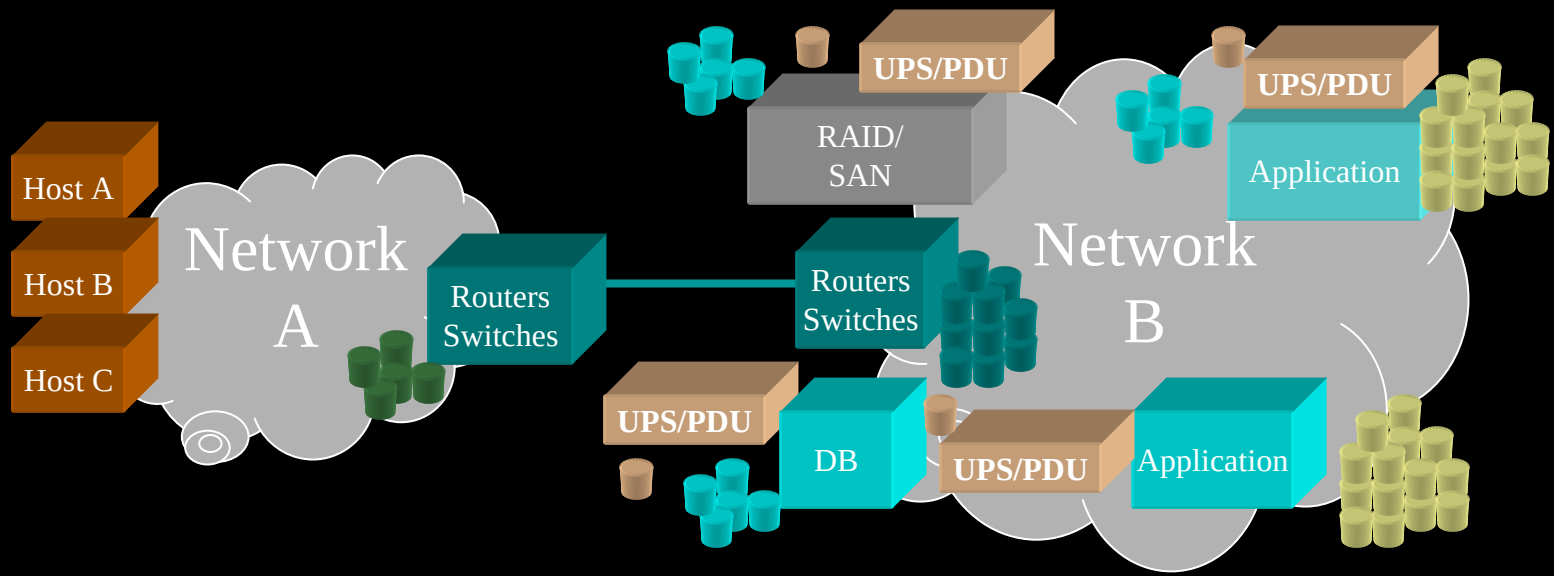
- Peer network routers/switches
- RAID and SAN devices
- Application servers
  - CRM, Payroll, patient records
- Maybe:
  - Configuration problem
  - Resource contention
  - Intermittent device failure

An Illustration (3)

Present day manual process for resolution

- Map DNS/DHCP/IP address/MAC address
- Inspect historical network statistics on all devices in the path
  - Interface information: byte, packet and error counts
  - Device health: CPU, memory, power supply, etc.
  - Network flow records of devices in question
- Manually inspect logs/statistics on server and client applications and middleware systems

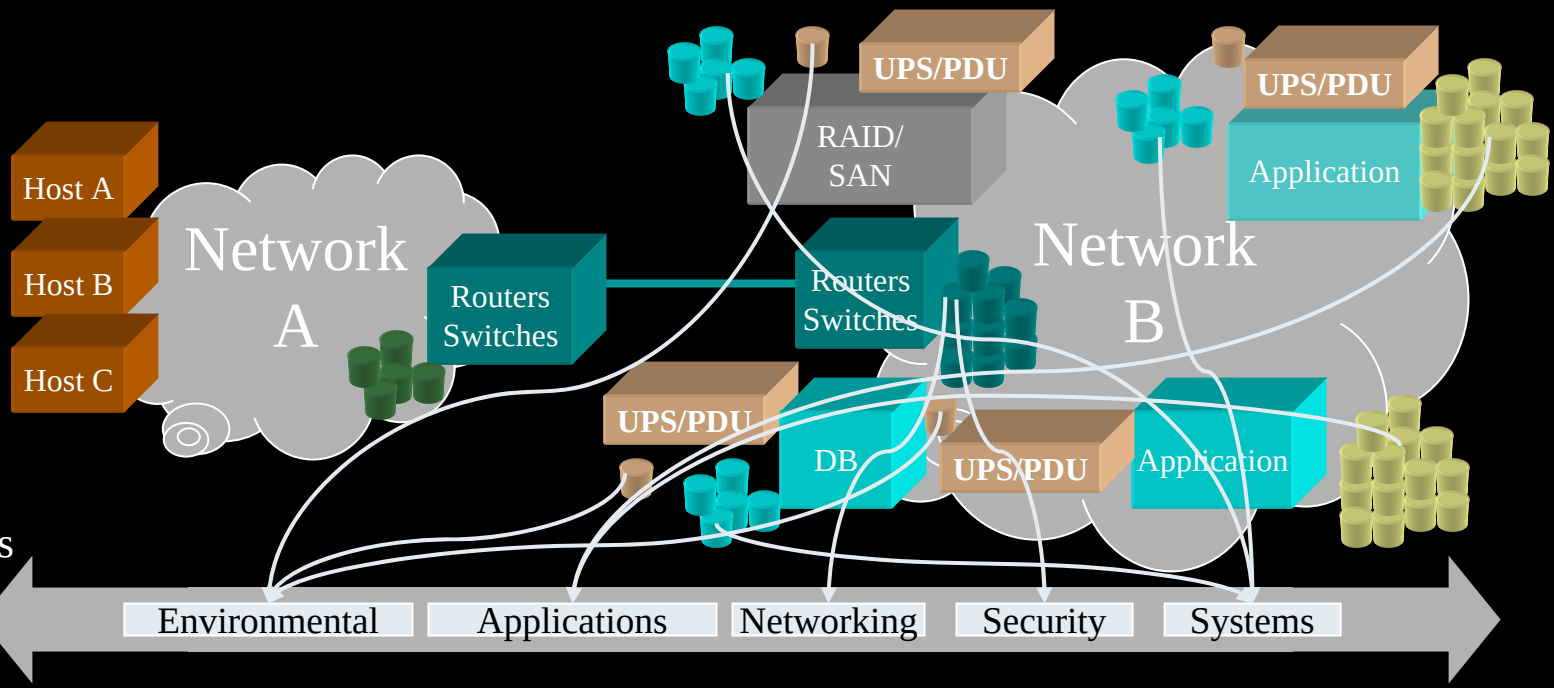
Separate Event Domains



Network Info
System Log Info
Application Info
Environmental Info

Carnegie Mellon

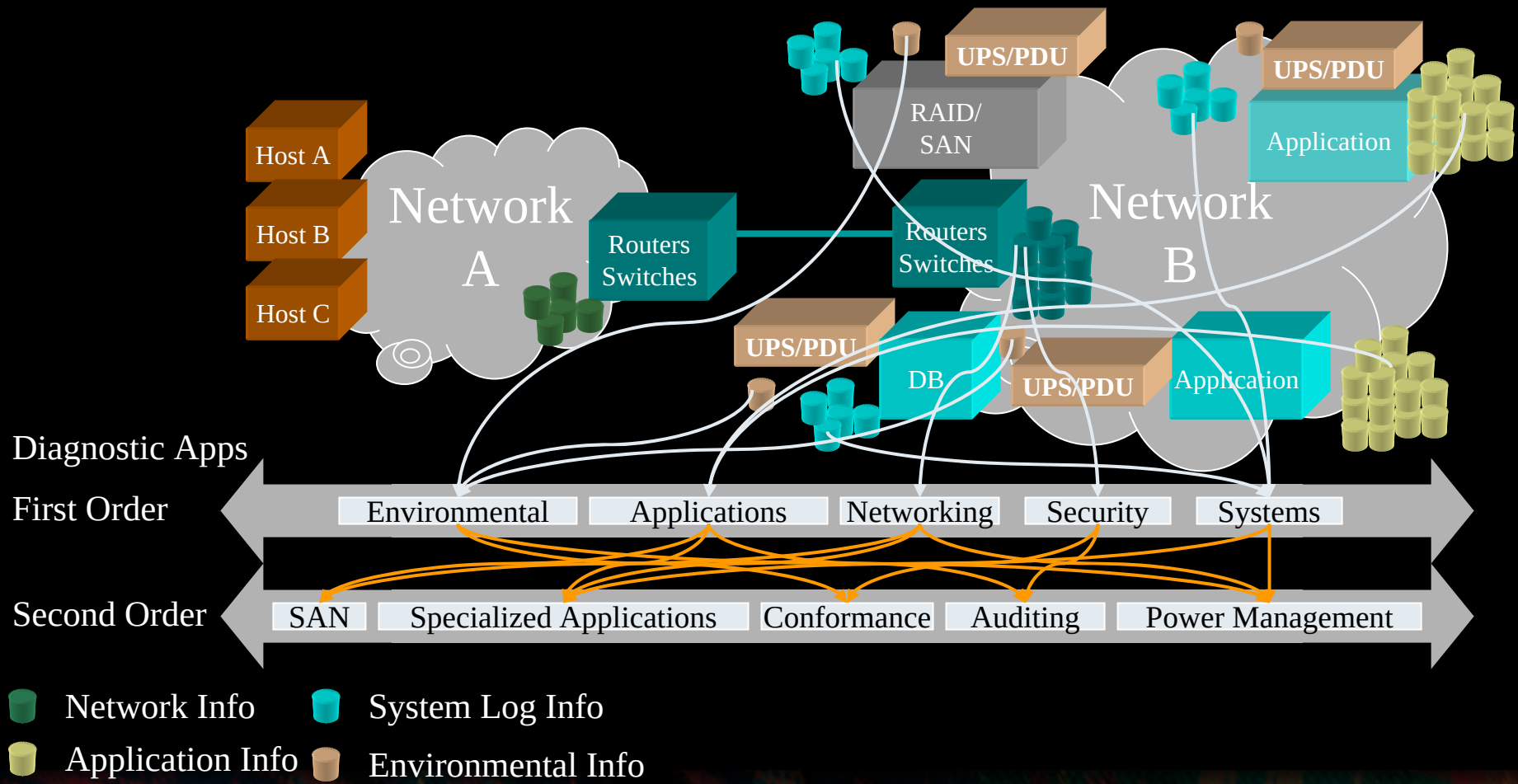
Collecting Event Domains



Network Info
System Log Info
Application Info
Environmental Info

Carnegie Mellon

Integrating Event Domains



System Administrator Questions

- Why was the payroll application slow?
- The redundant power supply failed on the RAID (using the SAN) caused by a PDU failure and the RAID was cycling between write through and write back mode.

Thinking about the Problem

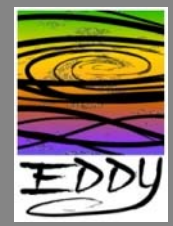
[A Layered Architecture for Diagnostic Infrastructure]

1. Sensing Technology
   - State, transaction info, whatever…the ability to collect anything
2. Diagnostic Data Orchestration
   - Data acquisition/normalization/transport, getting the:
     - Instrumentation data you want
     - In the format that you need
     - Where you want it
3. Diagnostic Information
   - Generic translation and statistical methods
   - Simple event correlation, visualization, longitudinal pattern analysis
   - Data Lifecycle (must be policy driven)
4. Domain-specific Diagnostic Analytics
   - Detailed analyses, situational diagnosis, specialized UI's
   - Significant automation of the domain and implementation autonomics

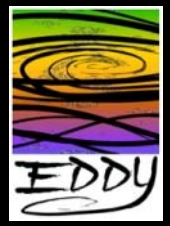
Thinking about the Problem

[A Layered Architecture for Diagnostic Infrastructure]

1. Sensing Technology
   - State, transaction info, whatever…the ability to collect anything
2. Diagnostic Data Orchestration
   - Data acquisition/normalization/transport, getting the:
     - Instrumentation data you want
     - In the format that you need
     - Where you want it
3. Diagnostic Information
   - Generic translation and statistical methods
   - Simple event correlation, visualization, longitudinal pattern analysis
   - Data Lifecycle (must be policy driven)
4. Domain-specific Diagnostic Analytics
   - Detailed analyses, situational diagnosis, specialized UI's
   - Significant automation of the domain and implementation autonomics



Carnegie Mellon



EDDY Capabilities

[Orchestrate Data and Create Generic Information]

Enable correlation

- Common Event Record (CER) – a way to format event information to make it easier to process
  - TTL, timestamp, observation point, normalizer location, event type, GUID, severity, user defined tags
  - Extensible payload, leverage domain data formats

Provide transport

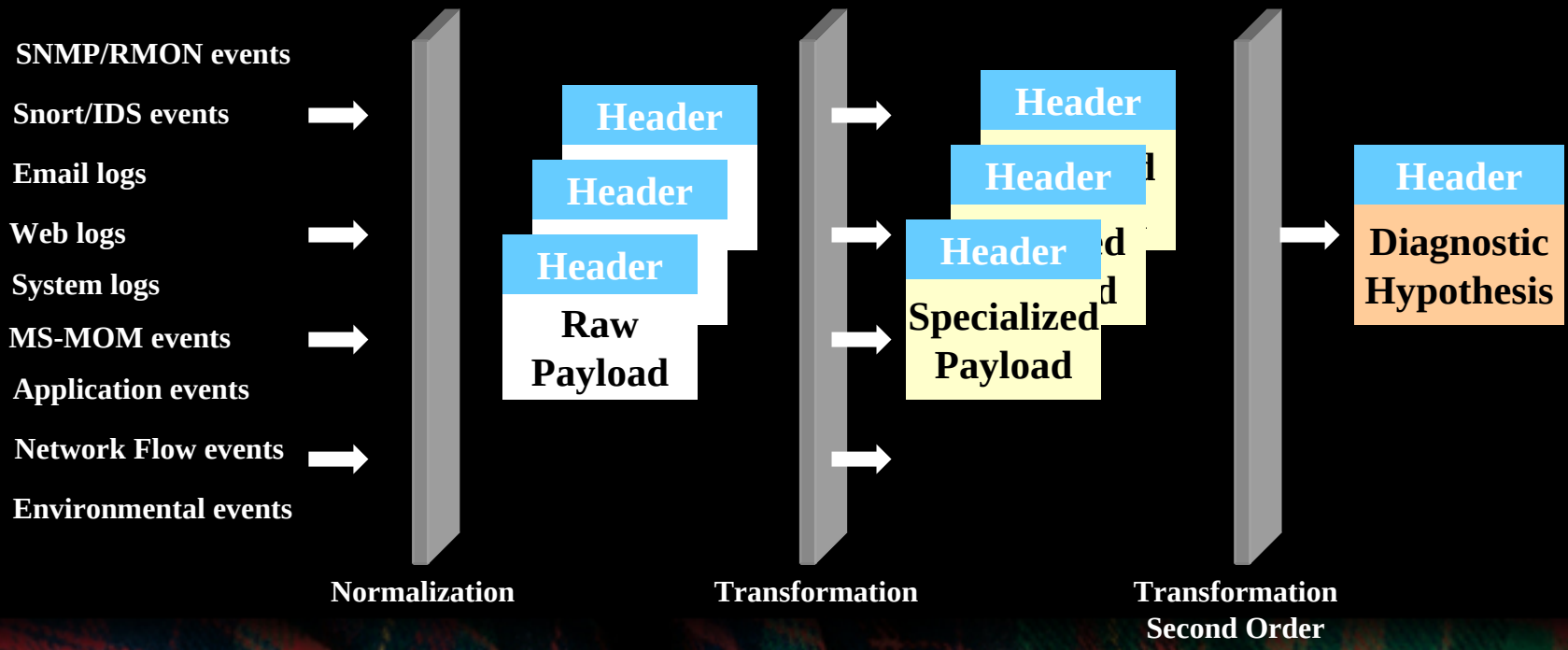
- Diagnostic Backplane – a way to move CERs around to make it easier to automate processing
  - High performance and XMPP

Some simple event orchestration methods

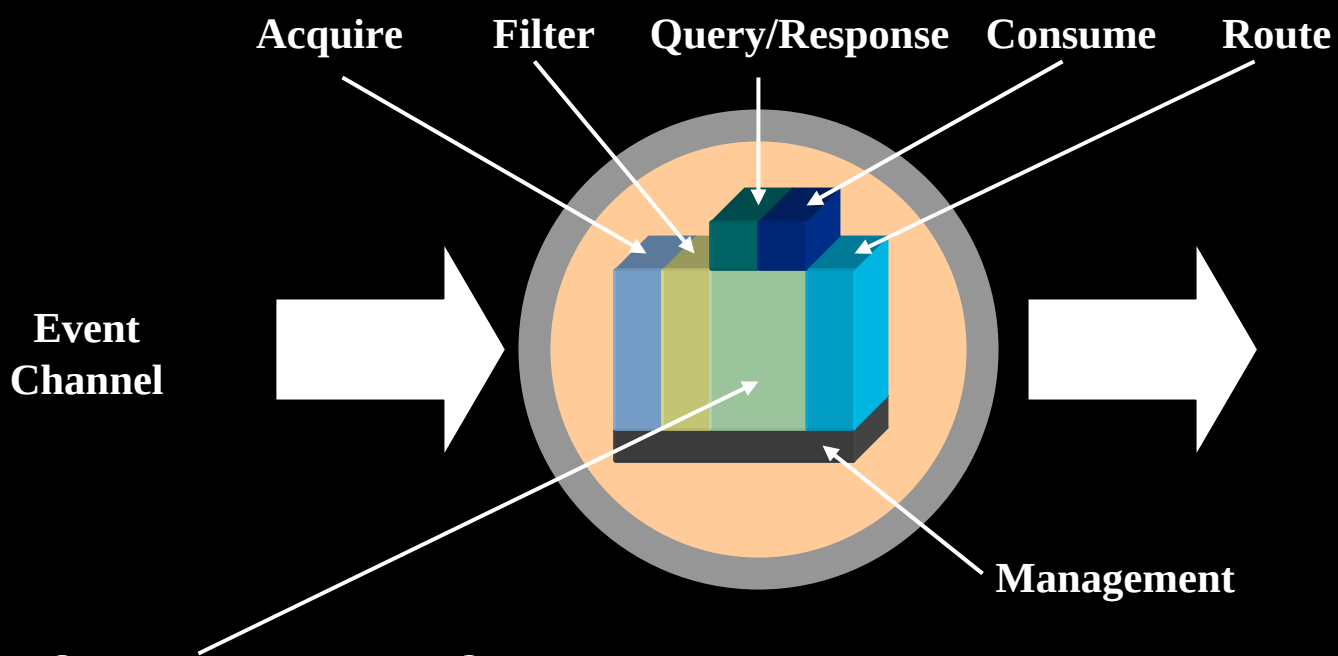
- Normalize, transform, visualize, store, anonymize

EDDY Extensibility and Scalability

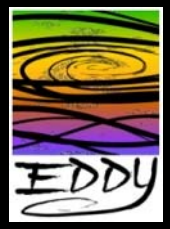
You don't need all the data, pick off only what you need...



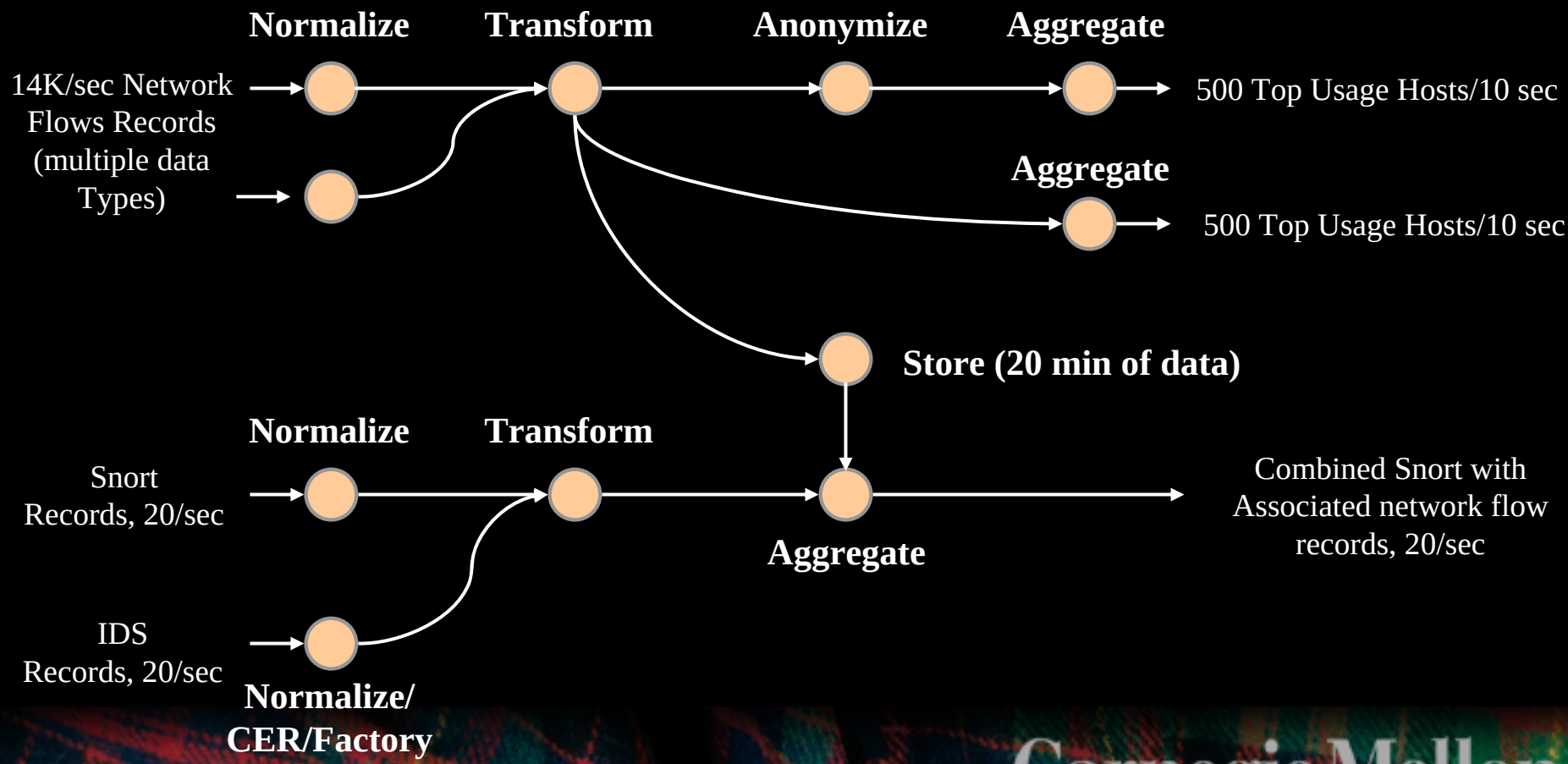
EDDY Agent Appliance Anatomy



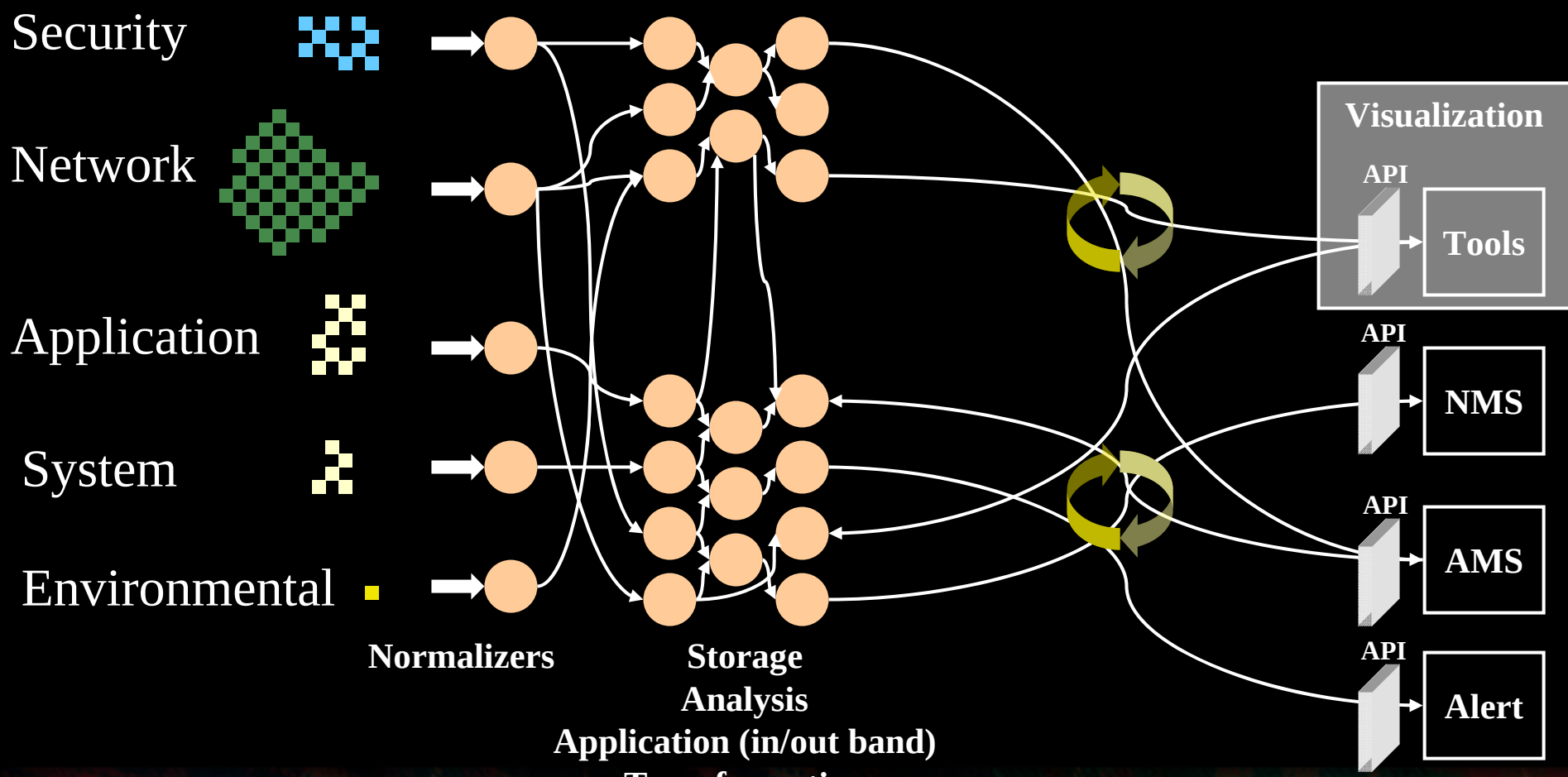
Transform: to name few....
Anonymize , store, archive, morph (many flavors), join, transfer (external communication), aggregation, normalize, etc.

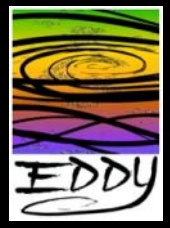


Appling domain agnostic methods to domain specific solutions



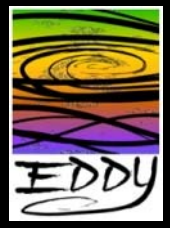
EDDY Agent Framework Functionality (filter/action/route)





What EDDY is

- Architecture for cross domain diagnostics
- An enabling technology that provides
  - Event ledger
  - Dissemination and correlation infrastructure,
    - Afford research access to event data (anonymized)
  - A development platform for diagnostic research
    - Domain specific
    - Domain agnostic



What EDDY is not

- A system/network/application/security management platform
- The analysis engine, it enables the analysis to happen with domain expertise

Carnegie Mellon CyDAT

Cyber-center for Diagnostics Analytics and Telemetry

- Architecture and Standards
  - Design and define specifics for the IT Diagnostic Plane
  - Standards for data format and transport
- Open Source Prototype
  - A reference implementation for experimentation with the Diagnostic Plane
- Observatory
  - Leverage a large-scale event facility at Carnegie Mellon for engineering and research collaboration on real data
  - Computing Services provides data, needs engineering analyses
  - Facilitate data export to other researchers
  - Research on structure and behavior of the Diagnostic facility
  - Engage corporate collaboration

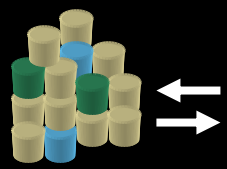
Carnegie Mellon

Observatory Service Infrastructure

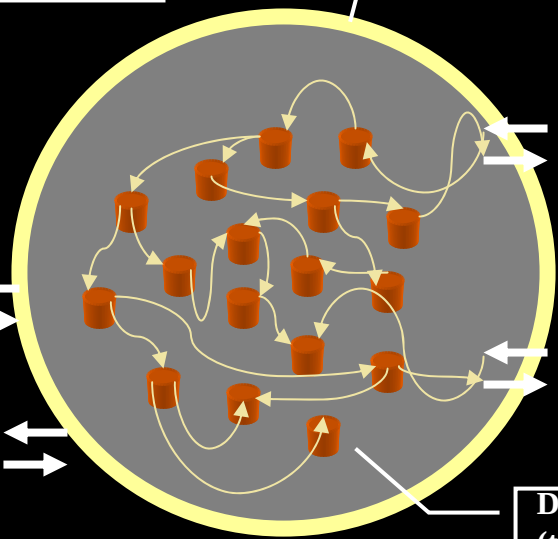
- Data flow:
  - publish/subscribe (EDDY/XMPP) <1K/s
  - high performance push API (EDDY/HP) 14K/s+
- Query: under development
- Common data format: EDDY Version II

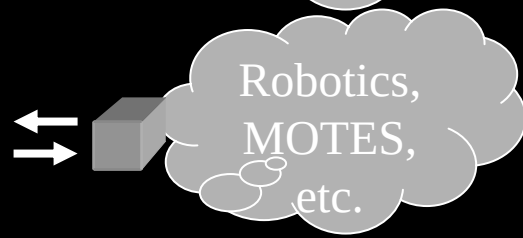
Real data from experimental sensor networks

Real data from production enterprise systems, networks, and environmental information. Custom probes, syslog aggregation, network flows



Researcher Analysis Applications





Data orchestration services (translation, storage, etc.)

Data orchestration/storage agents

Data orchestration/storage agents

Application/System Events

Network Events

Security Events

Carnegie Mellon

Observatory Services

- Multi-Campus Infrastructure
  - Import services
    - Sources: researcher sensors, computing services data from servers and networks, from facilities management
  - Access to data (stored and streams) – leverage Andrew authentication/authorization
  - Data Translation
    - Anonymization, aggregation, domain agnostic and domain specific from researcher requests
    - Leverage CyDAT Observatory compute cluster
  - Enforcing policies “in concert” with ISO and IRB
- Global Campus
  - Collaborative data access to global campus

Want to Learn More?

- Web sites
  - www.cmu.edu/eddy
  - www.cylab.cmu.edu/research/cydat.html
- Principal Investigators
  - Chas DiFatta (chas@cmu.edu)
  - Mark Poepping (poepping@cmu.edu)

Carnegie Mellon

Questions/Comments

The Case for Comprehensive Diagnostics

CyDAT - Cyber-center for Diagnostics, Analytics and Telemetry

Chas DiFatta (chas@cmu.edu)
Dan Klein (dvk@lonewolf.com)
Mark Poepping (poepping@cmu.edu)

Carnegie Mellon