ArcSight™

Scaling ArcSight Deployments

Hector Aguilar
Marylou Orayani
Christian Beedgen

Who are we?

- Hector Aguilar
  - VP of Network Products
  - Connectors, NSP
- Marylou Orayani
  - Senior Development Manager
  - Logger
- Christian Beedgen
  - Chief Architect, Engineering Director
  - ArcSight Manager

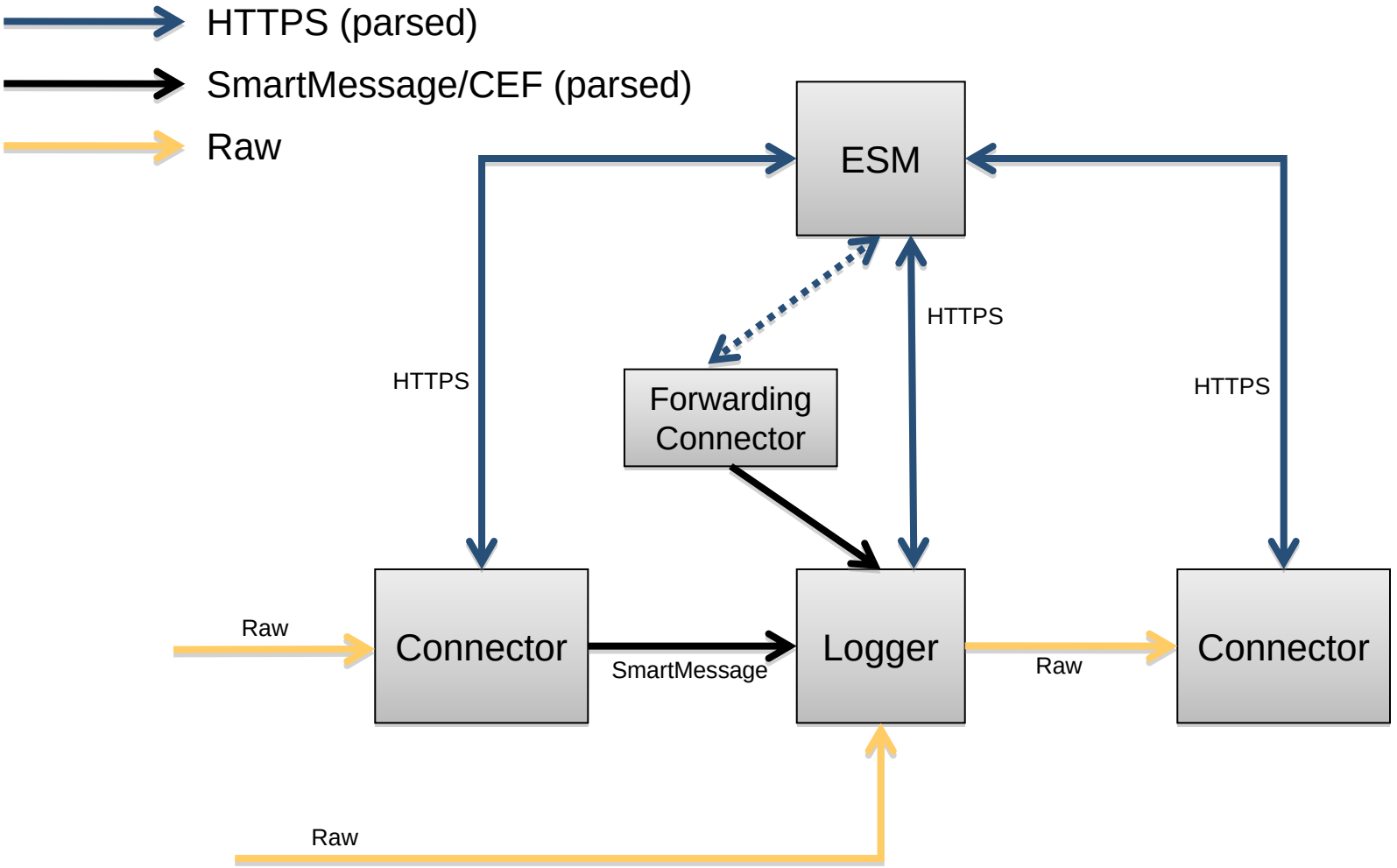
Who are you?

- Customers?
  - Which products?
  - For how long?
- Prospects?
- Why did you come to this session?

Agenda

- This is a panel discussion
- We have a couple of motivating slides
- This is a two-way discussion about
  - The ArcSight ecosystem
  - Deployment options

Dataflow



Transports

- HTTPS
  - This is just the classic agent-to-manager protocol
  - This includes heart-beating and the ability to send messages
- SmartMessage
  - Secure transport that encapsulates CEF
  - CEF is Common Event Format transported over Syslog
- Raw
  - Whatever the actual data source is
  - Logger can receive raw data via syslog (UDP & TCP) and via files

Logger in front of ESM

- EPS rate is very high; higher than ESM can handle typically
- Event receipt and storage is of paramount importance
- Subset of events is needed for correlation
- Can potentially loop correlation events back into Logger

Logger behind ESM

- Event rate is no more than ESM can ingest
- Forwarding Connector feeds Logger
- Events have addtl ESM-specific information
- Includes correlation events easily
- Logger as archive for ESM