CERN'S COMPUTER SECURITY OPERATIONS CENTRE

LIVIU VÂLSAN

PRE-GDB, 12TH OF JULY 2016

System Design

Sources of data
- IDS systems: Bro, Snort/Suricata
- System logs
- Netlog
- Execlog
- Active Directory / Krb
- Single Sign On logs
- Web logs
- DNS logs
- Automatic scan results

Flume sources

Malware Information Sharing Platform
- Intelligence framework

Sources of information
- Network database
- Active Directory
- DNS / DHCP
- Geo IP lookups

Spark
- Data enrichment
- Aggregation Correlation
- Stream processing

Kafka
- Central data backbone

Alerting
- SIEM

Flume sinks

Spark
- Batch & custom jobs

HDFS
- Long term storage

Solr
- Real time indexing

Hue & Custom CLI
- Visualisation