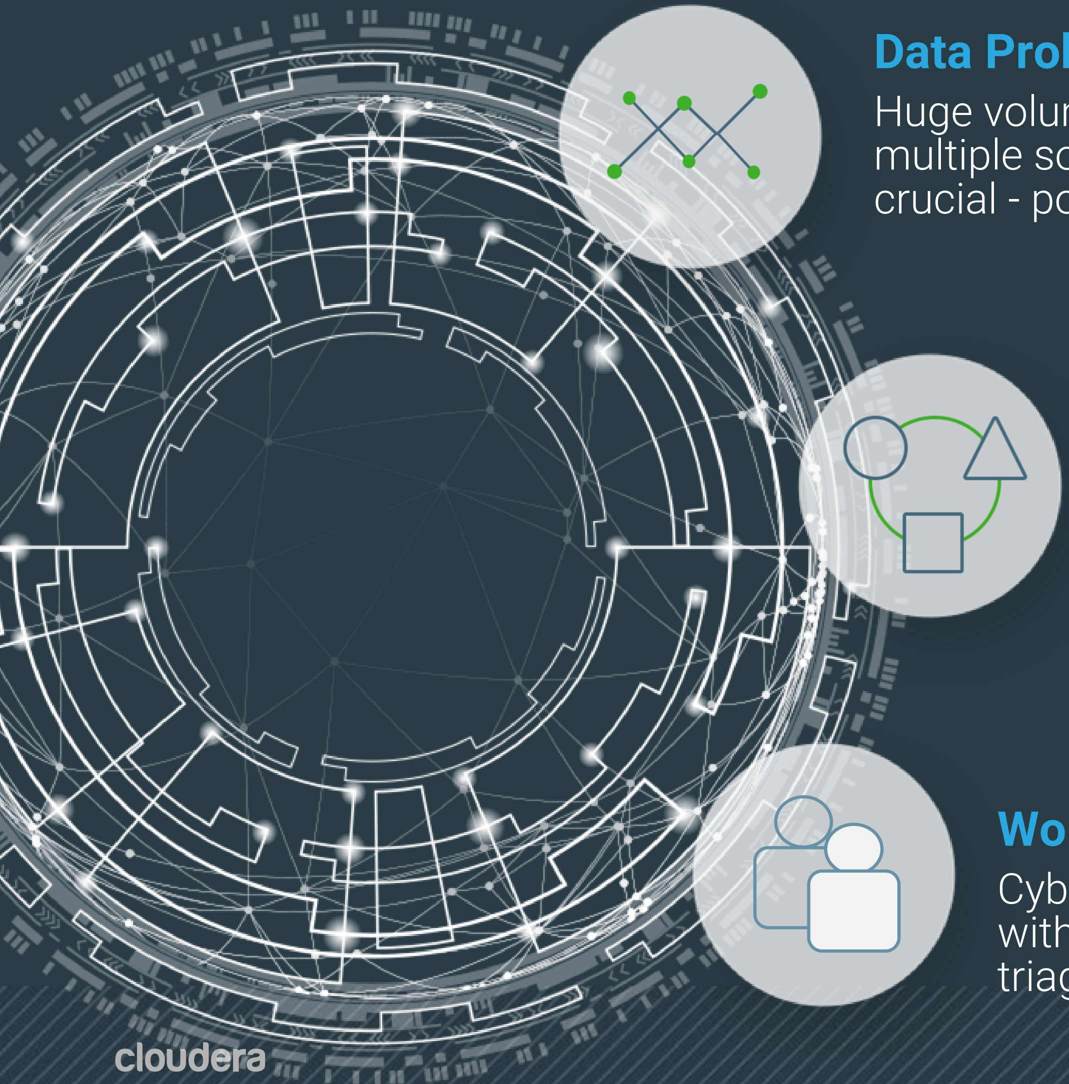
10 YEARS JETSECURITY

CONFERENCE 2019

Cyber security at scale: solving the skills gap with real time data science

Simon Elliston Ball, Product Manager, Cloudera

CYBERSECURITY IS A BIG DATA PROBLEM



Cloud, kubernetes and containers driving log expansion in customers beyond capacity

Data Problem

Huge volumes, inconsistent data from multiple sources, & real-time context is crucial - post-hoc investigation is too late

Complexity Problem

Too many point solutions, too many dashboards, too hard to correlate data across silos

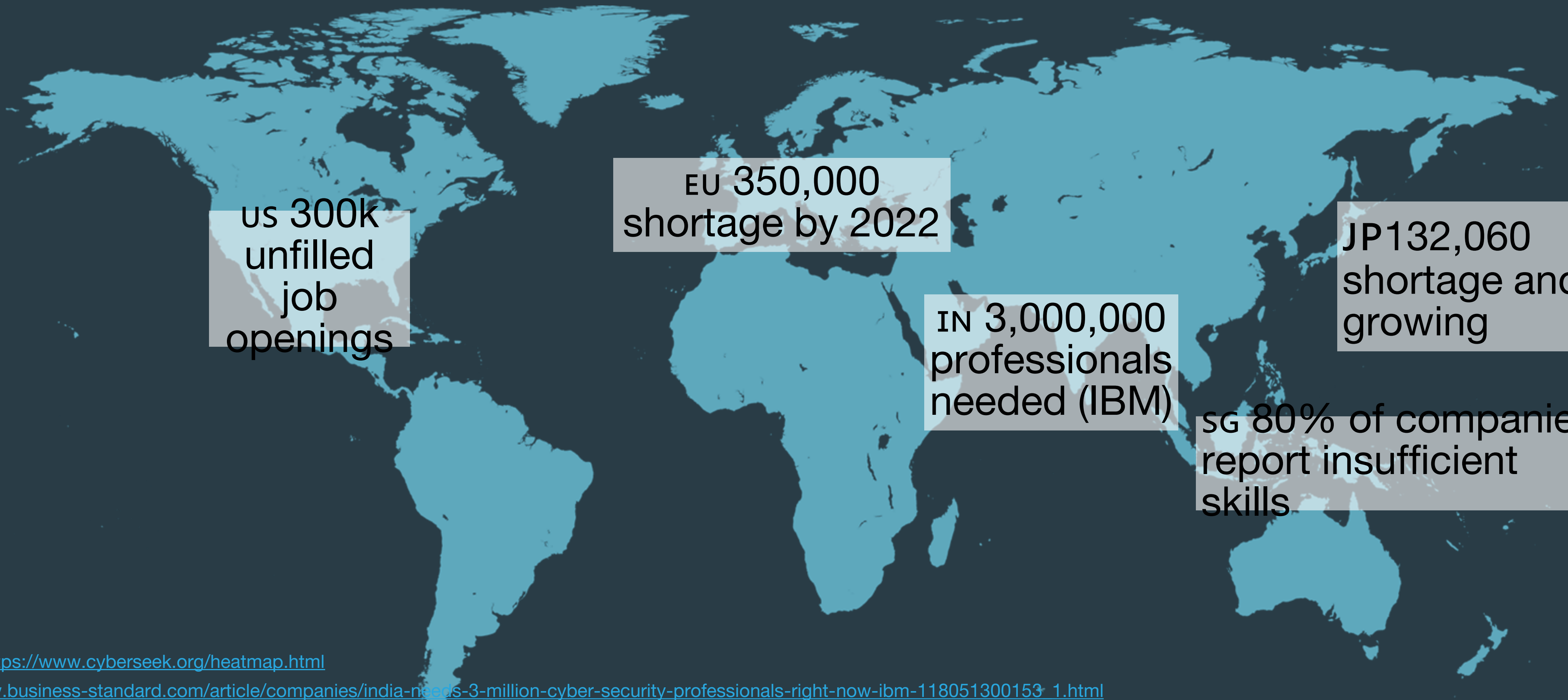
Workload Problem

Cybersecurity staff overwhelmed with too many alerts, spend all day triaging events | alerts lose meaning

DATA IN CYBERSECURITY IS A **BIG DATA** PROBLEM

CYBERSECURITY IS A PEOPLE PROBLEM: SHORTAGES

Need people efficiency



US 300k unfilled job openings

EU 350,000 shortage by 2022

IN 3,000,000 professionals needed (IBM)

JP132,060 shortage and growing

SG 80% of companies report insufficient skills

Sources: https://www.cyberseek.org/heatmap.html
https://www.business-standard.com/article/companies/india-needs-3-million-cyber-security-professionals-right-now-ibm-118051300153_1.html
https://www.ey.com/sg/en/newsroom/news-releases/news-ey-singapore-companies-confident-of-predicting-and-resisting-cyber-attacks
https://www.computerweekly.com/news/450420193/Europe-faces-shortage-of-350000-cyber-security-professionals-by-2022
https://researchcenter.paloaltonetworks.com/2017/05/cso-japan-aiming-close-cybersecurity-skills-gap-tokyo-2020/

WHY CLOUDERA CYBERSECURITY PLATFORM?

Increased SOC Efficiency

with integrated threats streams into single integrated view and toolset

Rapid Threat Detection

through real-time security data ingestion from disparate sources

Reliable Insights

Use **ALL** the data: long term historical data collection, enriched by ongoing data collection and correlations

Automated Intel. Detection

intelligent behavior-driven threat detection based on behavior profiles and machine learning

Value on the journey

Offload SIEM Costs

High speed sources

Longer term retention

Threat hunting

Compliance

Better Outcomes

Data science to reduce rules maintenance cost

Behavior profiles automate baselining

Hunt the APTs

Advanced ML and AI

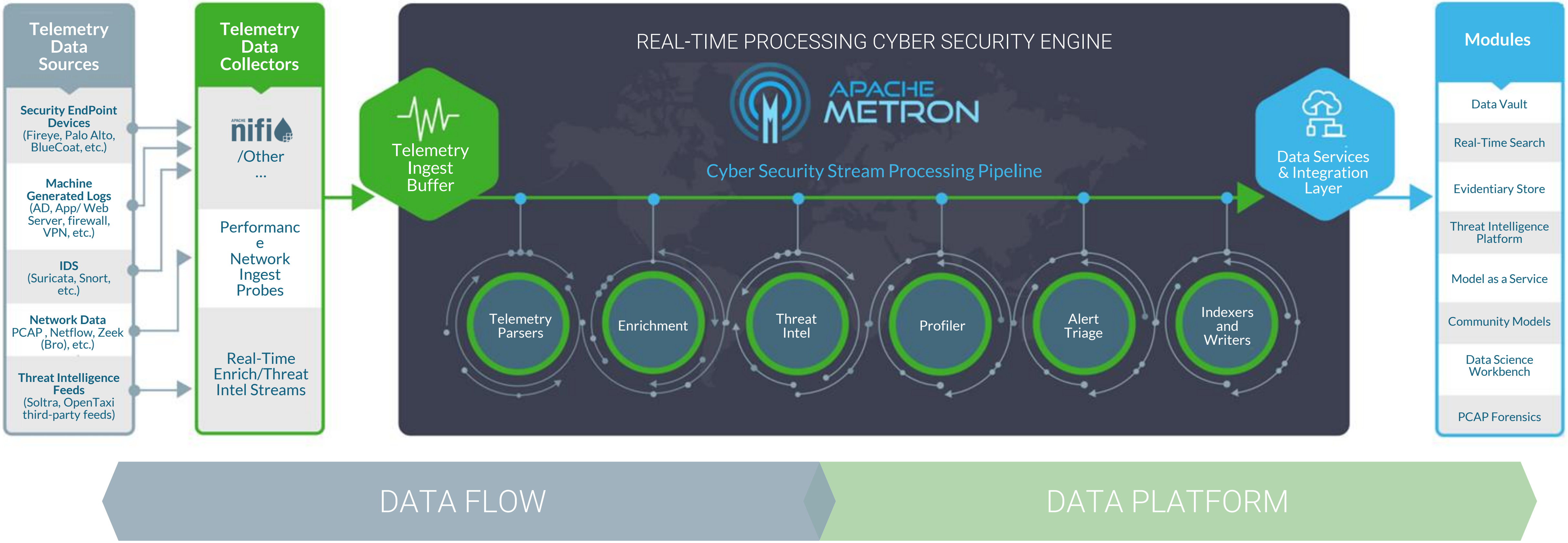
Better detection

Automation of analyst activity

Assist and prioritize scarce analyst resources

SOLVING CYBERSECURITY AT SCALE

An architecture for real-time cybersecurity analytics


Telemetry Data Sources
Security EndPoint Devices (Fireye, Palo Alto, BlueCoat, etc.)
Machine Generated Logs (AD, App/ Web Server, firewall, VPN, etc.)
IDS (Suricata, Snort, etc.)
Network Data PCAP , Netflow, Zeek (Bro), etc.)
Threat Intelligence Feeds (Soltra, OpenTaxi third-party feeds)
Telemetry Data Collectors
nifi /Other …
Performanc e Network Ingest Probes
Real-Time Enrich/Threat Intel Streams
REAL-TIME PROCESSING CYBER SECURITY ENGINE
APACHE METRON
Telemetry Ingest Buffer
Cyber Security Stream Processing Pipeline
Telemetry Parsers
Enrichment
Threat Intel
Profiler
Alert Triage
Indexers and Writers
Data Services & Integration Layer
Modules
Data Vault
Real-Time Search
Evidentiary Store
Threat Intelligence Platform
Model as a Service
Community Models
Data Science Workbench
PCAP Forensics
DATA FLOW
DATA PLATFORM

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!