

RSA[®]CONFERENCE2014

FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

Share.
Learn.
Secure.

Capitalizing on
Collective Intelligence

Security Business Intelligence— Big Data for Faster Detection/Response

SESSION ID: STU-R02B

Stacy Purcell

Security Architect
Intel/IT



Legal Notices



This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Intel and the Intel logo are trademarks of Intel Corporation in the U.S. and/or other countries.

* Other names and brands may be claimed as the property of others.

Copyright © 2013, Intel Corporation. All rights reserved.



 #RSAC

RSACONFERENCE**2014**

A taste....



10 min.

FIVE HUNDRED IOCs



365 days

TWO TRILLION EVENTS



1 day

TWO HUNDRED BILLION EVENTS



Agenda



- History & Philosophy
- Architecture
- Big Data
- Fast Detection Use Cases
- Challenges & Next Steps



Perspective



Former employee pleads guilty to stealing Intel documents

April 9, 2012

Former Intel engineer Biswamohan Pani pleaded guilty Friday in U.S. Federal Court in Massachusetts to stealing Intel chip manufacturing and design documents shortly before he went to work for AMD in 2008.



Purpose



Provide a set of detective controls and decision support systems to help balance the gaps in our preventative controls and enable new security controls to minimize the increasing risk to the enterprise.

Types Of Cyber Events Analyzed

- Brute Force Login Attempts
- Identity And Personal Data Theft
- Denial Of Service Attacks
- Malicious Proxy Activity
- Server Anomalies
- Endpoint Malware Detection



#RSAC

RSA CONFERENCE 2014

Privacy



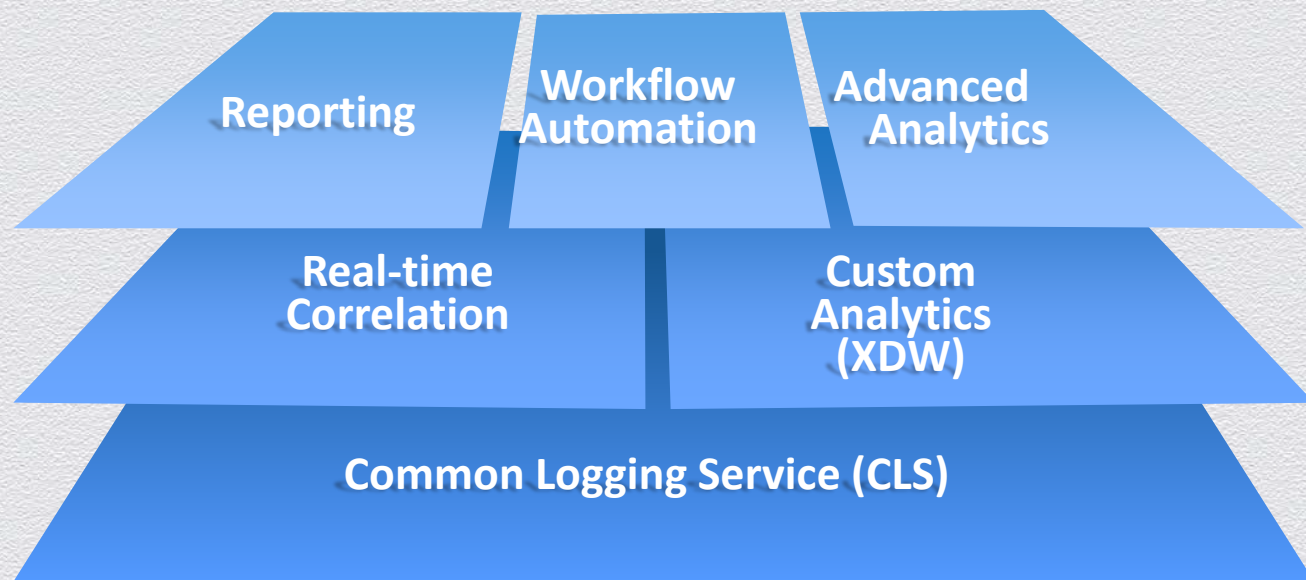
Evolving from focusing on individual SBI use cases to focusing on entire SBI system, data lifecycle and governance model

- ◆ Established privacy controls framework that defined common requirements for system components and data sources
- ◆ Privacy plans established for specific use cases and SBI data sources
- ◆ Use limited to Cyber Security Threat Management & Incident Response
- ◆ New use cases and access must be approved by CSO/CPO and Chief Privacy & Security Legal Counsel
- ◆ Developing a tiered privacy control framework as SBI evolves

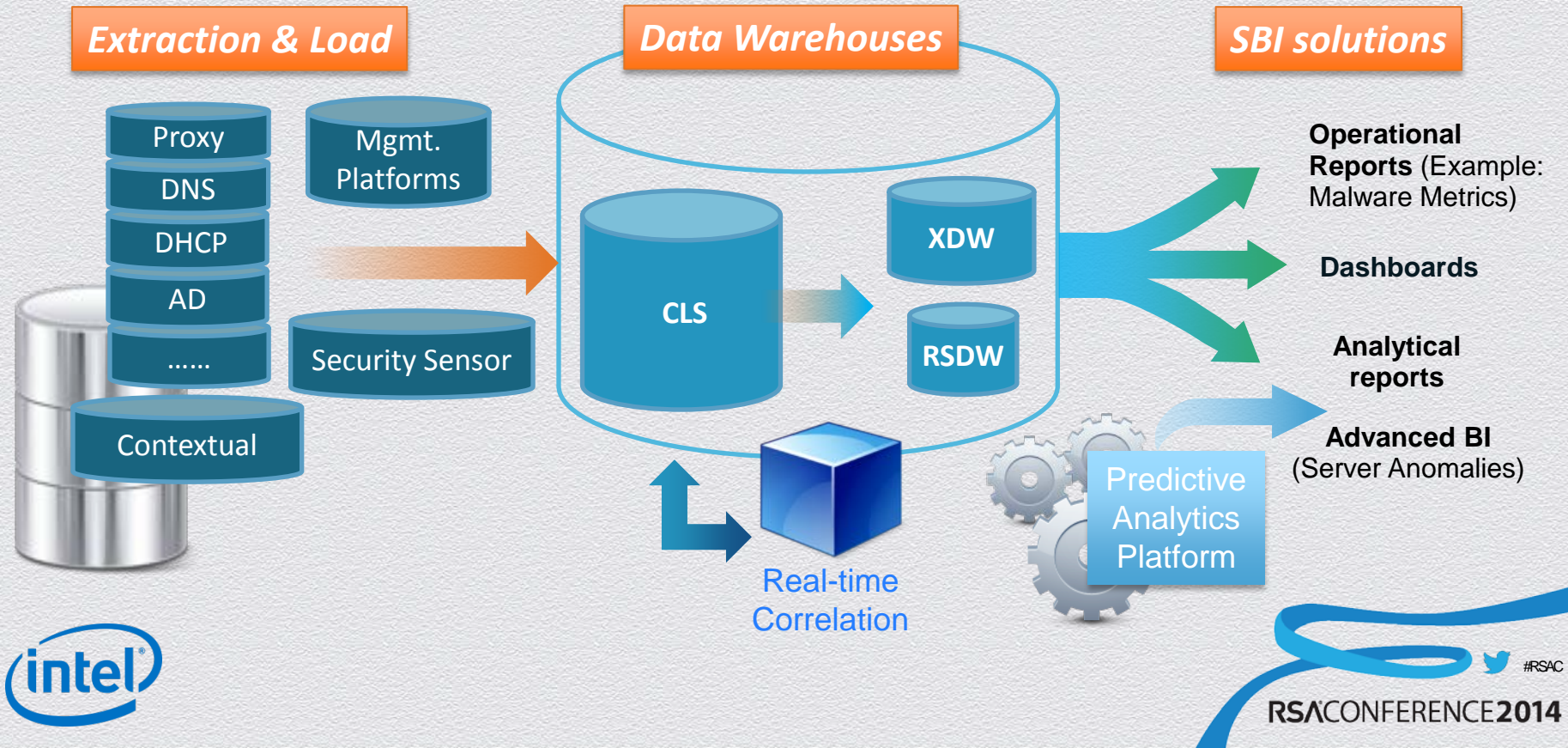


RSACONFERENCE2014

SBI Capability Stack



SBI Suite of Capabilities



SBI 2013 Core Capability by the Numbers

Real-Time Correlation

Compute and Storage

- 316 cores
- ~80TB storage*

Events

- 70M events/day
- 30 day rolling window
- 22 event sources

Reporting

Workflow Automation

Advanced Analytics

Real-time Correlation

Custom Analytics (XDW)

Common Logging Service (CLS)

XDW/ Custom Analytics

Compute and Storage

- 104 cores
- ~128TB storage*

Events

- ~700M new events/day
- ~60M events scanned/hour
- 60-90 day rolling window
- 4 event sources plus 9 contextual sources

Compute and Storage

- 236 cores
- ~3.5PB storage*

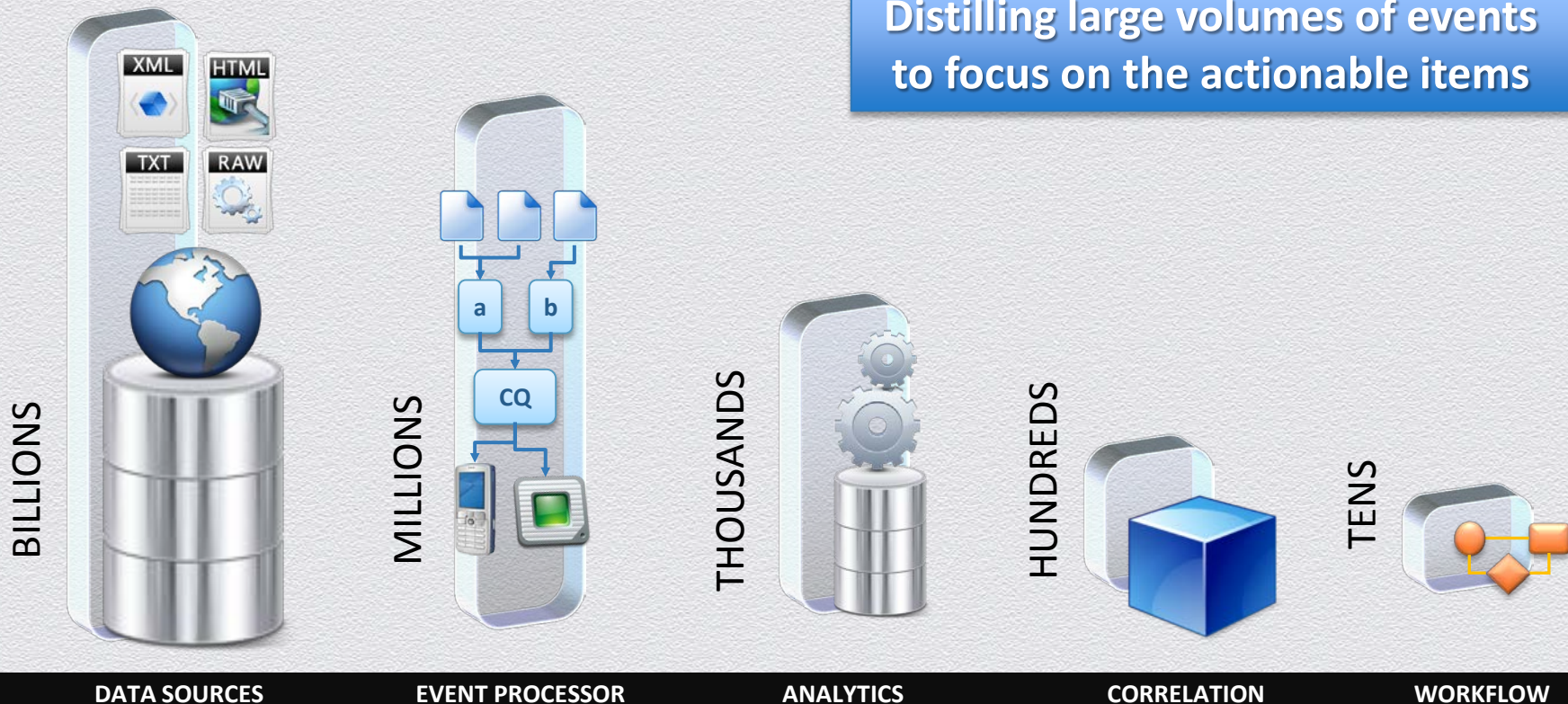
Events

- 7 Billion events/day
- 2Trillion+ total events
- 1 year rolling window
- 23 event sources

* Storage numbers assume compression with 4X typical for CLS and 10X for RTC



Scaling for Big Data



SBI Value

Real-Time Correlation

New Sources/ New Rules

- Access Protection/ AV
- Proxy: Malicious Sources
- Proxy: Outbound Data/Botnets
- OSINT

Reporting

Workflow Automation

Advanced Analytics

Real-time Correlation

Custom Analytics (XDW)

Common Logging Service (CLS)

XDW/Custom Analytics

Malware Metrics

- DSS reports malware

Server Anomalies

- Regular external communication

AAA

- My Security Alerts
- Uncovered significant "IT Hygiene" issues

External Presence, Internal Cloud, Authentication, Connectivity, Brute Force Login, Elevated privilege logins, Identity Theft, DoS, Server Anomaly, DNS and DomainFlux connections, Endpoint Malware Detection

Response

- 99% TPT reduction
- 1 Tool, 1 Process
- C2 IOC match <5 Minutes
- Fact Table/Order 1 Search



Security BI Risks & Challenges

- **Privacy – more data at risk**
- **Potential mining of the data for IP theft or harm**
- **Big data requires new big data tools**
- **Big data can slow forensics**
- **As devices get smaller more data pushed to the cloud**





Next Steps

- **My Security Alerts**
- **Database Activity Monitor**
- **Comprehensive Coverage**
- **Rapid Response**



#RSAC

RSACONFERENCE2014

Getting Started



- **Start small**
- **Start focused**
- **Grow value based on design goals**
- **Build a team**

Every organization has a different risk posture,
all organizations require customized analysis.



Resources



Rethinking Information Security to Improve Business Agility

Executive Overview

Use of this approach has already helped us deliver innovative solutions to challenging use cases while actually reducing risk.

To enable rapid adoption of new technologies and usage models—and provide protection in an evolving threat landscape—Intel IT has embarked on a radical five-year redesign of Intel's information security architecture.

We believe this architecture, designed to support key initiatives such as IT consumerization and cloud computing, represents a novel approach to enterprise security. It provides more flexible, dynamic, and granular controls than traditional

containing less-valuable data and allowing broader access. Communication between zones is controlled and monitored; if one zone is compromised, this prevents the problem from spreading to other zones.

Fast Threat Detection with Big Data Security Business Intelligence

- To reduce risk, IT must rapidly correlate event log data
- We are able to selectively monitor 1.5 billion directory service events per day
- Our new solution enables large-scale log management and custom analytics

Intel IT's new Security Business Intelligence (BI) platform incorporates common logging service (CLS), real-time correlation engine, and analytics platforms to deliver faster detection and response to ability to implement custom analytics solutions enables our security team to distill specific event logs from over 6 billion events recorded daily. This provides improved compliance, better protection of high-risk assets, and response to advanced persistent threats.

After operating a near-real-time correlation engine on smaller data sets, we saw the need for a comprehensive log management solution.

WHITE PAPER
Privacy Principles
January 2014




Applying Privacy Principles in a Rapidly Changing World

As new technology and data uses strain traditional privacy guidance, Intel recognizes the enduring value of this guidance and seeks ways to implement recognized privacy principles flexibly and effectively.



Learn more about Intel IT's initiatives at: www.intel.com/IT

 #RSAC
RSA CONFERENCE 2014