Monitoring GDPR Compliance with Splunk

David Hendrawirawan & Rishita Rai | Deloitte & Touche LLP

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

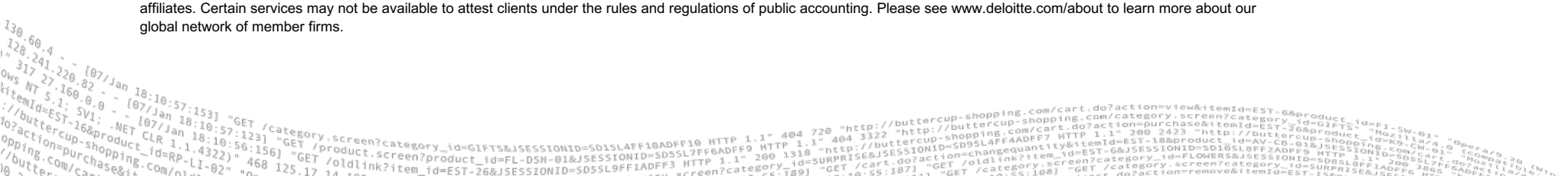
Disclaimer

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte shall not be responsible for any loss sustained by any person who relies on this or presentation.

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. In the United States, Deloitte refers to one or more of the US member firms of DTTL, their related entities that operate using the “Deloitte” name in the United States and their respective affiliates. Certain services may not be available to attest clients under the rules and regulations of public accounting. Please see www.deloitte.com/about to learn more about our global network of member firms.



splunk> .conf18

Introductions

David Hendrawirawan, CISA, CIPP/E
Advisory Senior Manager
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

Rishita Rai, Splunk Certified Architect
Advisory Senior Consultant
Deloitte Risk and Financial Advisory
Deloitte & Touche LLP

EU General Data Protection Regulation (GDPR)

Introduction

splunk> .conf18

The Big Picture

In the digital economy, business leaders face increasing scrutiny by the public and regulators about their organization's ability to strategically handle & safeguard data from misuse

Regulators are raising the bar

- US Federal Communications Commission (FCC): user consent / permission for broadband data sharing
- GDPR & California Consumer Privacy: individual data rights
- State of Missouri: anti-trust investigation on an internet search platform

Customers are expecting more

- Harvard Business Review (HBR): monetary value of data trust & transparency
- Data privacy vs. losing income – which do Americans prefer?
- Company offers free credit monitoring after major breach

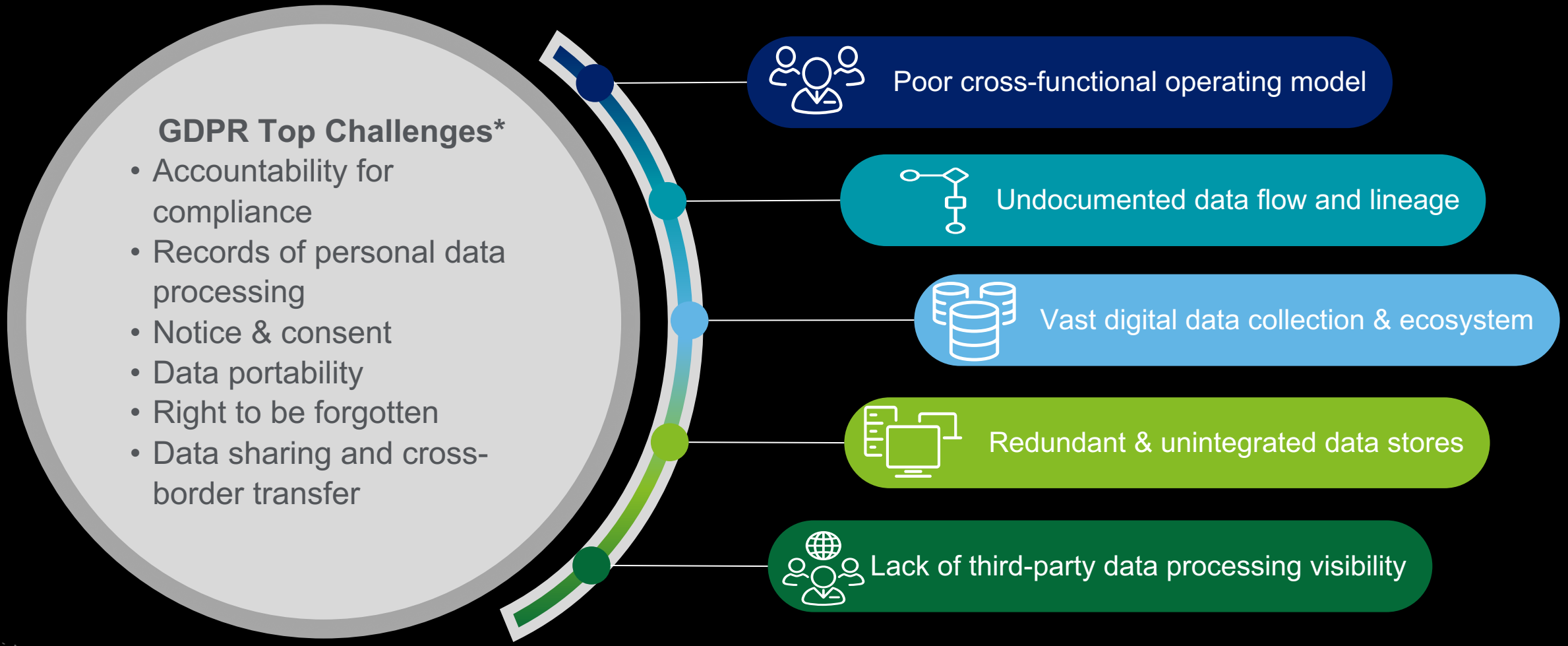
Businesses treats data as strategic

- Tech companies: ramping up suspicious accounts monitoring & removal
- Social media: improving robust privacy settings
- Three-quarters of data on marketing databases are useless post-GDPR

See a list of references in Appendix

Most Common GDPR Challenges & Data Management

Strategic management and governance of data assets across the enterprise becomes competitive advantage to tackle the root causes of the top challenges presented by GDPR and other privacy and data protection rules.

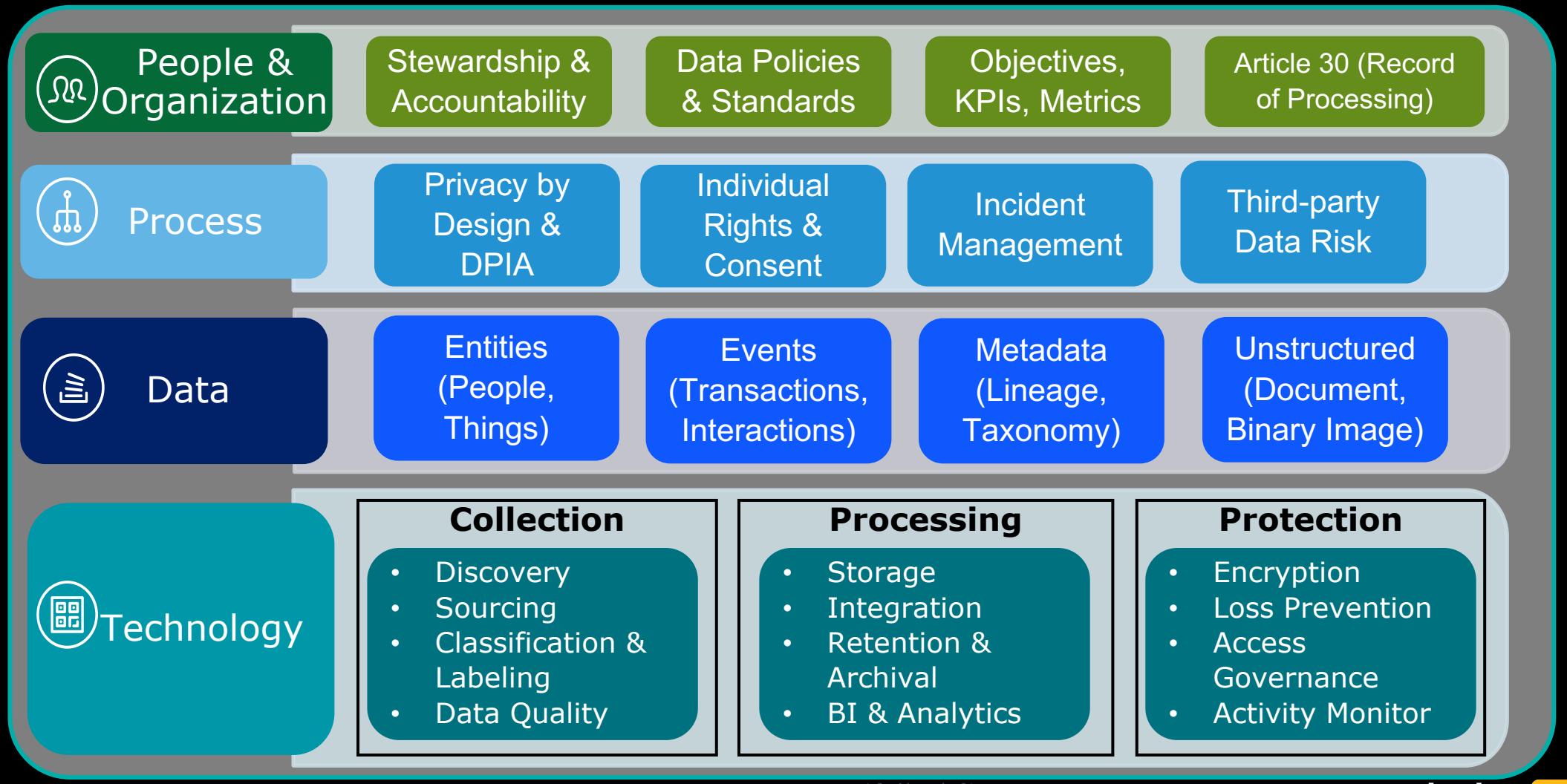


* Based on IAPP Annual Privacy Governance Report and the Deloitte General Data Protection Regulation Benchmarking Survey

splunk> .conf18

Holistic Approach to Address and Comply GDPR

A holistic approach involves cross-functional operating model and capabilities across business analytics, information security, and data management to effectively and efficiently meet GDPR requirements.



splunk> .conf18

GDPR Monitoring Areas & Sample Use Cases

Information Governance

- Metadata Management
- Data Flow & Lineage
- Data Handling & Retention

Data Security & Protection

- Data Access Controls (DAC)
- Data Activity Monitoring (DAM)
- Data Loss Prevention (DLP)
- Data Remediation

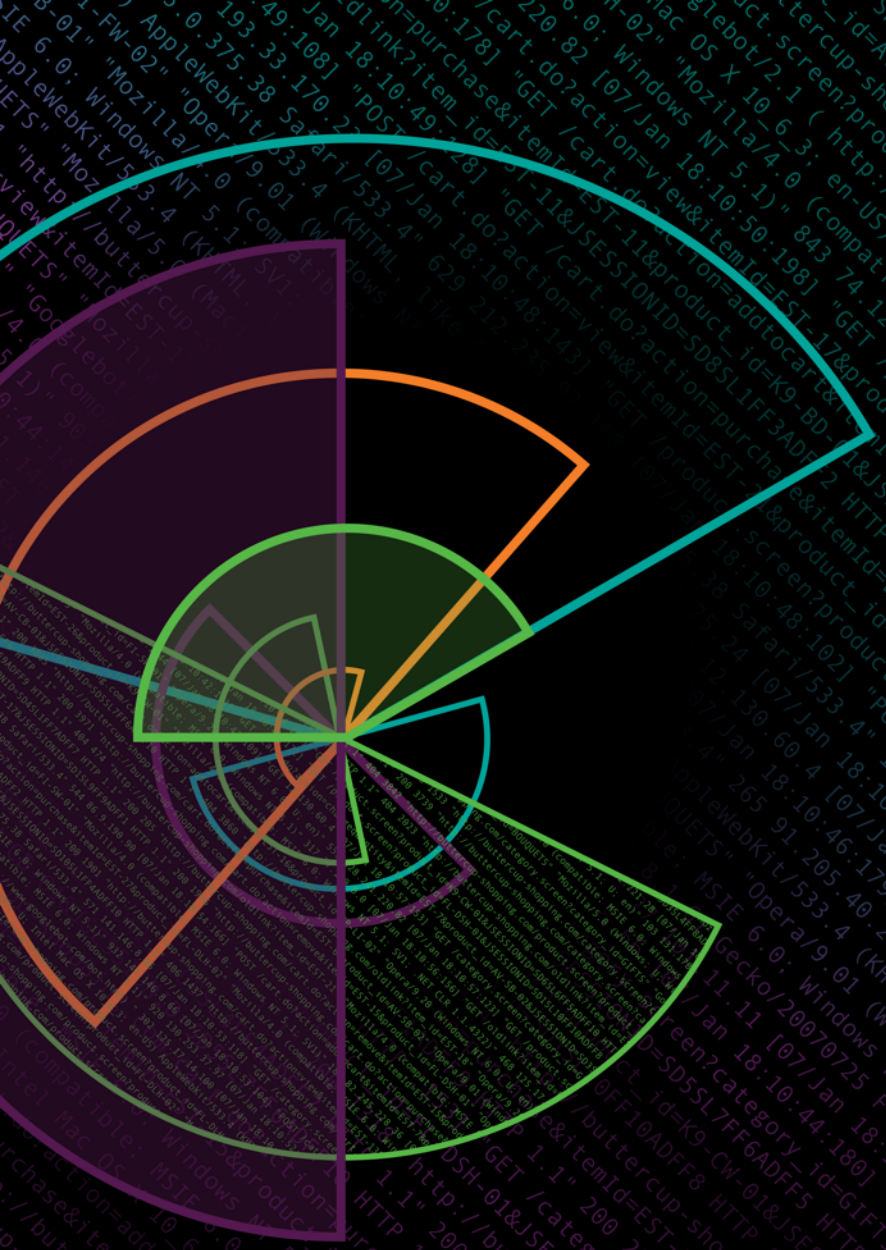
Individual Privacy Rights

- Consent Record
- Data Subject Rights

Sample Use Cases

- Database Change Management
- Data In-Transit Monitoring
- Stale Data Disposal
- Exfiltration & Breach Detection
- Suspicious Behavior Analysis
- Asset & Vulnerability Management
- Consent Revocation Monitoring
- Data Erasure Assurance

splunk> .conf18



Use Cases

Case Studies

splunk> .conf18

1. Database Change Management

- **Leverage metadata catalog or data governance tool**
  - Effective to document data flows / maps for GDPR Article 30*
  - Enable discovery, monitoring, and enforcement of standards and policy

- **Database platforms: track creation and modification of dataset schemas and tables**
  - Monitor Database Definition Language (DDL) and application programming interface (API) services schema modifications
  - Correlate approved datasets in metadata catalog with database logs

Data Sources

- ***Database audit trail logs (DDL)***
- ***Reference metadata & lineage***

Search Correlation Logic

- ***Normalize Database Audit logs (DDL)***
- ***Search for DDL actions***
- ***Correlate approved data lineage with actions***

Risk Addressed

- ***Ensure data discoverability & adherence to policies***
- ***Detect unauthorized activity of sensitive Personal Information (PI)***
- ***Validate data erasure and disposal***

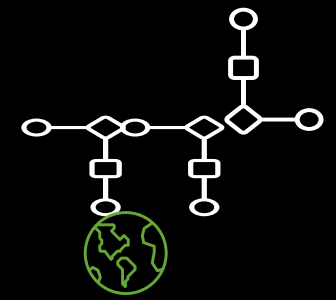
*As part of GDPR Record of Processing Activities

splunk> .conf18

2. Data In-Transit Monitoring

- **Metadata catalogs can document data lineage and flow across the enterprise**
  - Identify sensitive data flow in source-to-target map / lineage

- **Monitor data flow and processing lineage to detect exposure of sensitive data**
  - Network DLP can stop / send alert for sensitive information exfiltration
  - Track APIs and services account creation
  - Identify authorized actions, accessible IP address and ports



Data Sources

- ***Data lineage and flow from metadata catalog***
- ***DLP events***
- ***Middleware / API service accounts, user privilege details***

Search Correlation Logic

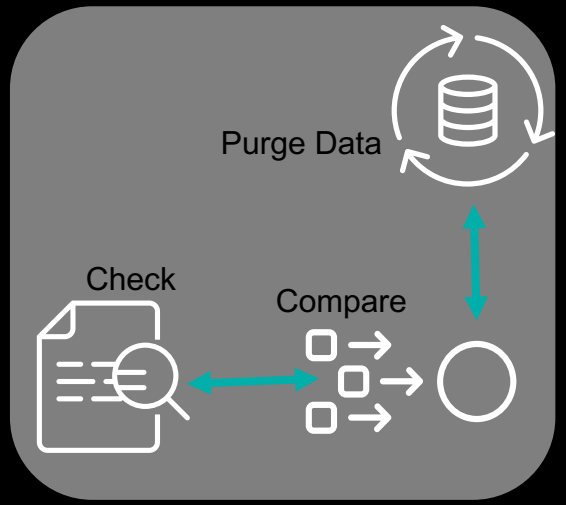
- ***Normalize sensitive data***
- ***Define in-transit or source-to-target maps***
- ***Correlate authorized data lineage & data flow indicators***

Risk Addressed

- ***Detect unauthorized or unprotected data transfer / exfiltration***
- ***Monitor data aggregation and transformation logic***

3. Stale Data Disposal

- **Prevent uncontrolled growth, reduce risk of leakage with retention policy**
  - Classify data in terms of subject, categories, origin, and processing purpose
- **Monitor unpurged / stale data in databases, file shares, and directories**
  - Utilize database record or table level metadata
  - Data Access Governance (DAG) tools for file and folder level activity metadata



Data Sources

- *Defined data classification, processing purposes, and retention requirements*
- *Database audit trail of record level metadata*
- *DAG log of file / folder level metadata*

Search Correlation Logic

- *Compare file / folder metadata with retention requirements and flag stale data sources*
- *Review last update time vs. retention period and determine purging*

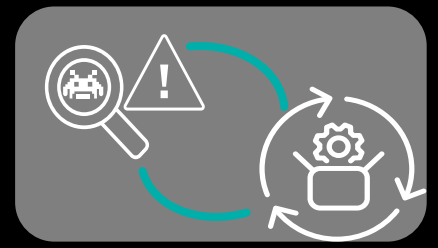
Risk Addressed

- *Identification of orphaned data*
- *Timely purging and destruction of stale data*
- *Reduce cost of storage and risk of data leakage*

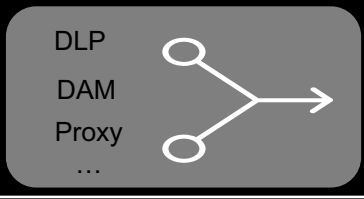
splunk> .conf18

4. Data Exfiltration & Breach Detection

- **Data leakage & breach detection, prevention, and impact analysis require multi-pronged solution:**
  - Network & proxy traffic logs analysis
  - DLP and DAM analysis
  - Encryption*, rights management, obfuscation, anonymization
  - Metadata catalog and tagging / digital signatures – enhance discoverability



- **Correlate logs from multiple solutions in centralized storage & analytics**



Data Sources

- ***DLP & DAM alerts***
- ***Network traffic & proxy logs***
- ***Databases / field encryption settings***

Search Correlation Logic

- ***Normalize DLP and proxy data***
- ***Set relevant threshold***
- ***Continuously baseline the threshold for "normal" behavior***

Risk Addressed

- ***Timely detection and prevention of sensitive data leak***
- ***Ability to efficiently assess and contain data breach impact***

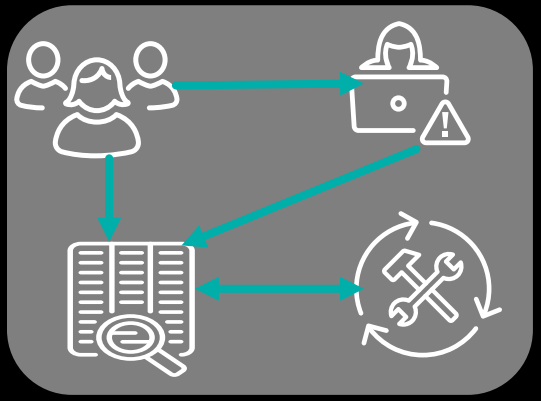
*Note: DLP & DAM must be architected to work with encryption

splunk> .conf18

5. Suspicious Behavior Analysis

- **Data theft and insider threats require sophistication beyond the baseline access controls**

- **User behavior analysis should be employed to correlate these attributes:**
  - Terminated employees or contingent workers access after termination
  - User access to high risk application, data & transactions
  - User security groups, and security zones
  - After hours or out of cycle activities in security zones



Data Sources

- ***Security Groups and geo zones***
- ***Master list of high risk data & transactions***
- ***Application activity data***
- ***Current active user and device signature info***

Search Correlation Logic

- ***Monitor non business hour activities***
- ***Track IP geo location***
- ***Correlate user to device signature for anomaly***

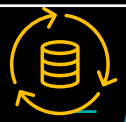
Risk Addressed

- ***Detect and prevent potential data theft by insider threat***
- ***Mitigate advanced and persistent threat from social engineers***

6. Asset & Vulnerability Management

- **Outdated patch, misconfiguration, or insecure software code in IT systems and Configuration**
  - Unable to prioritize and apply timely remediation to discovered vulnerabilities

- **Metadata catalog data should be triangulated with CMDB and network configurations**
  - Improve situational awareness and incident response readiness & enabling strategic prioritization
  - More timely resolution of vulnerabilities
  - Focused areas for Secure-System Development Life Cycle (S-SDLC) and Privacy by Design



Data Sources

- *IT Asset from inventory such as CMDB*
- *Sensitive data from data catalog*
- *Vulnerability scan details, dynamic and static analysis*
- *Network configuration*

Search Correlation Logic

- *Map IT Assets and sensitive data from CMDB and data catalog*
- *Identify clusters of sensitive data repositories in same network zones*
- *Correlate vulnerability scan to identify top Common Vulnerabilities and Exposures (CVE)*

Risk Addressed

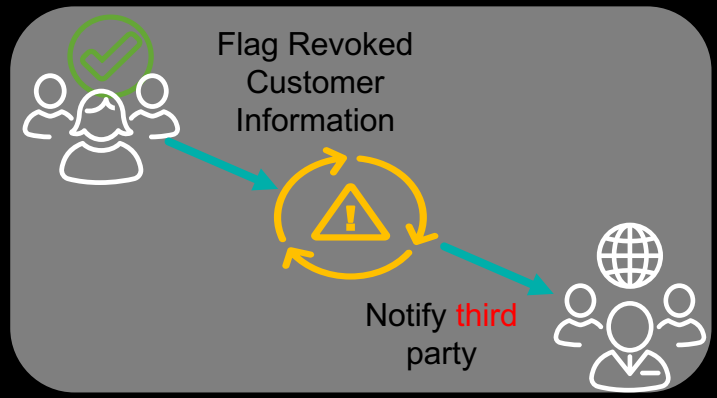
- *Proactively address strategic vulnerabilities*
- *Reduce risk of sensitive breach from systems and network zones*
- *Improve situational awareness and IR readiness*

* Note: CMDB is Configuration Management Database

splunk> .conf18

7. Consent Revocation Monitor

- **Individual customer may revoke consent for their data to be used for secondary purposes**
  - Companies are obliged to capture and record consent events
  - Marketing analytics and third-party eco-system must adhere



- **Splunk can be used to check for compliance by**
  - Alerting marketing application owners & third parties data processors
  - Flag when customer data are still processed / sent to marketing & third party

Data Sources

- ***Customer consent record and privacy preference repository***
- ***Application logs from marketing and third-party systems***

Search Correlation Logic

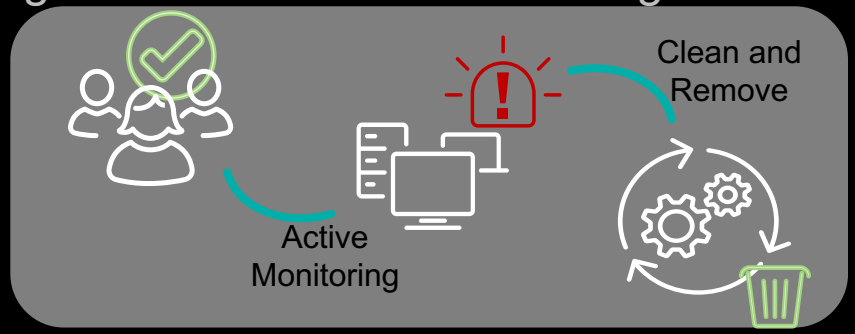
- ***Maintain a customer "black list"***
- ***Monitor application and database traffic data against the black list***
- ***Send alert to marketing and third party***

Risk Addressed

- ***Provide adherence to customer consent and individual rights***
- ***Customer confidence and trust in data handling process***

8. Data Erasure Verification

- **Right to be Forgotten = Fulfill a customer's request to erase their data within 30 days**
  - Good practice: Use single source of truth such as customer Master Data Management (MDM)
  - Run a script or a query to verify erasure and send a success / failure event to Splunk
  - Correlate erasure status against the customer MDM to gain further confirmation



Data Sources

- ***Erasure success / failure event from customer applications***
- ***Master record status from Customer MDM***

Search Correlation Logic

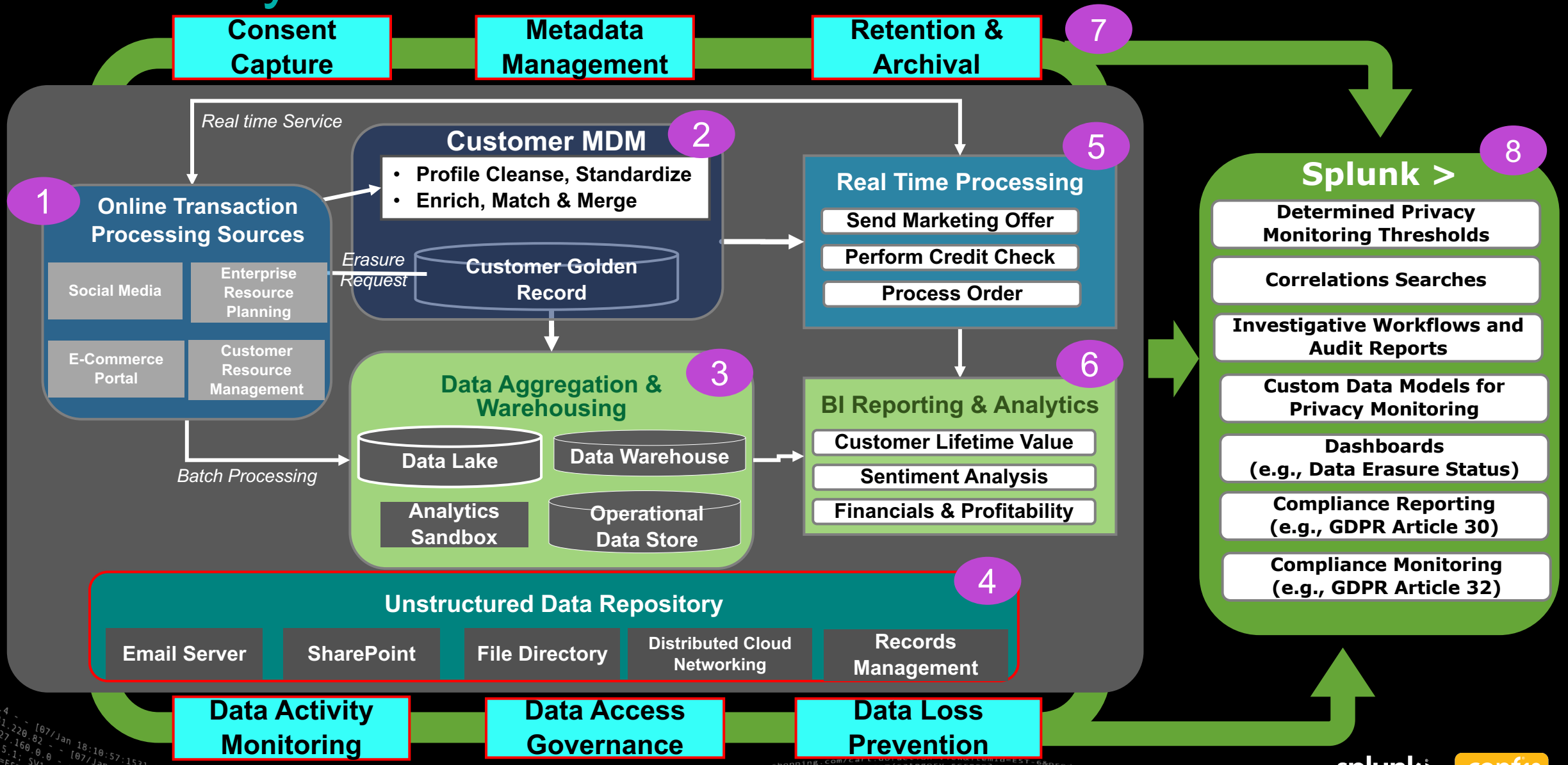
- ***Aggregate erasure event logs across multiple applications***
- ***Upon successful completion across all source systems, alert final status to Customer MDM***

Risk Addressed

- ***Provide adherence to customer consent and individual rights***
- ***Customer satisfaction and trust in data handling process***

splunk> .conf18

Privacy & Data Protection Architecture - *Illustrative*



splunk> .conf18

Appendix

This section contains links to useful information

List of References

1. https://inform.tmforum.org/data-analytics-and-ai/2016/10/monetizing-data-us-regulators-agree-new-data-privacy-rules/
2. https://techcrunch.com/2017/11/13/missouri-attorney-general-launches-an-anti-trust-investigation-against-google/
3. https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust
4. https://www.prnewswire.com/news-releases/study-finds-more-americans-concerned-about-data-privacy-than-losing-their-income-300211216.html
5. https://www.campaignlive.co.uk/article/gdpr-will-render-75-uk-marketing-data-obsolete/1441738
6. https://techcrunch.com/2017/09/19/twitter-claims-tech-wins-in-quashing-terror-tweets/
7. https://www.consumer.ftc.gov/blog/2018/01/equifaxs-free-credit-monitoring-time-ticking
8. https://www.usatoday.com/story/tech/2018/01/29/facebook-launch-privacy-center-ahead-eu-regulations/1071430001/

Thank You

Don't forget to rate this session in the .conf18 mobile app