ClearPoint
METRICS

Metrics Mashup

Ensuring the Success of Your Security Metrics Program

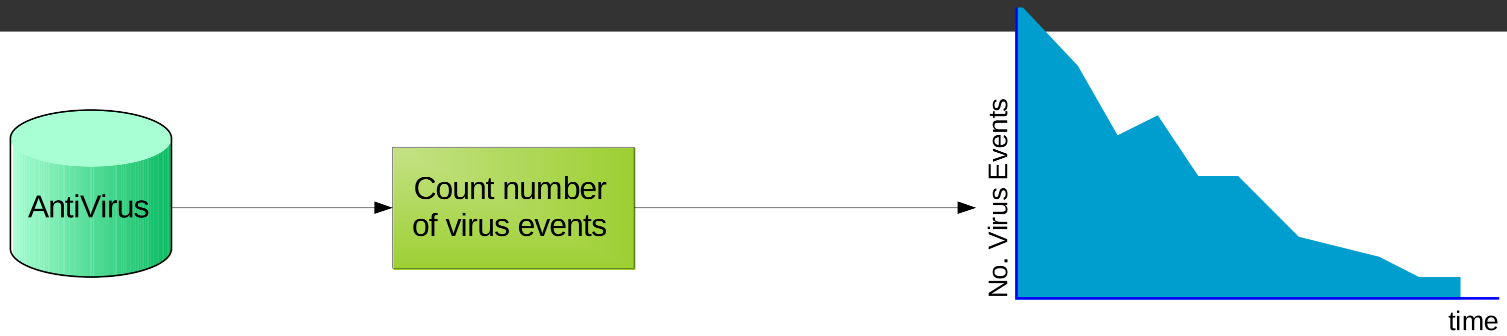
www.clearpointmetrics.com

Example – What a manager might want to know

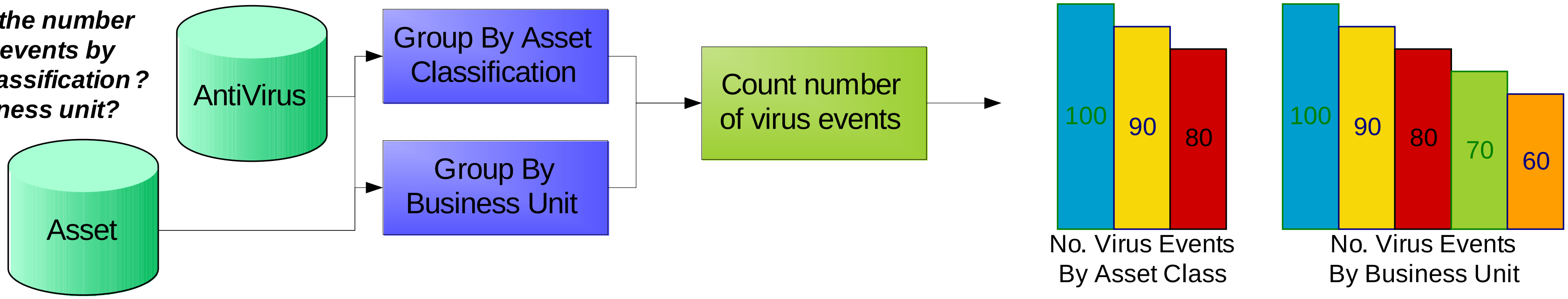
- What is the volume of virus events?
- What is the volume of virus events by asset class and business unit?
- How do we compare against others?
- Did these infections occur before or after signature updates?

Example – How we go about getting this information

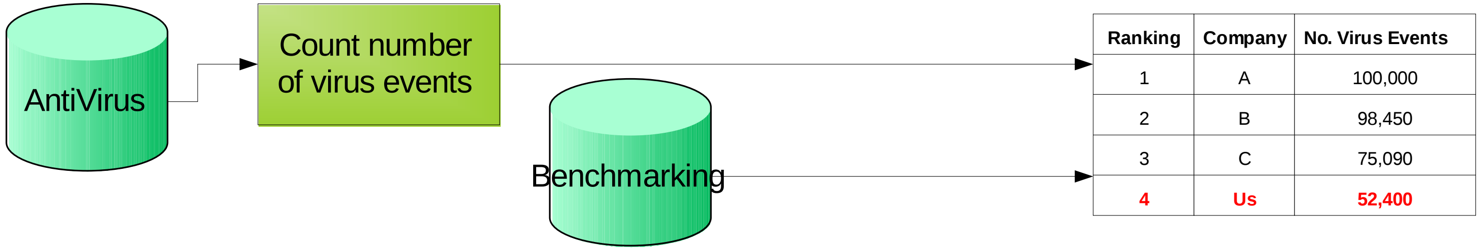
What is the number of virus events?



What is the number of virus events by asset classification? By business unit?

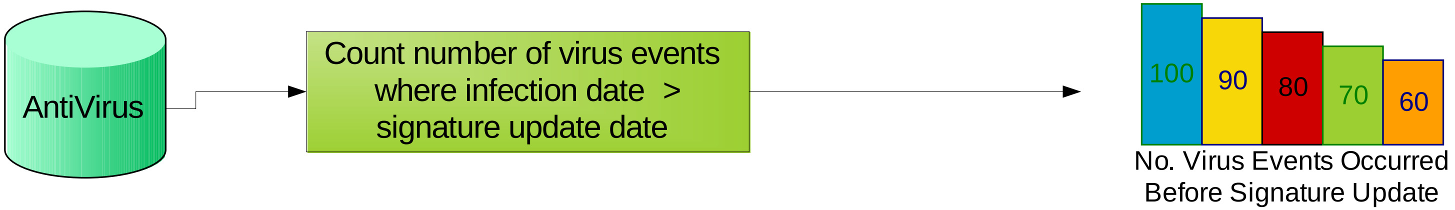

AntiVirus
Asset
Group By Asset Classification
Group By Business Unit
Count number of virus events
100
90
80
No. Virus Events By Asset Class
100
90
80
70
60
No. Virus Events By Business Unit

How do we compare against our peers?



Ranking	Company	No. Virus Events
1	A	100,000
2	B	98,450
3	C	75,090
4	**Us**	**52,400**

Did these infections occur before or after signature updates?

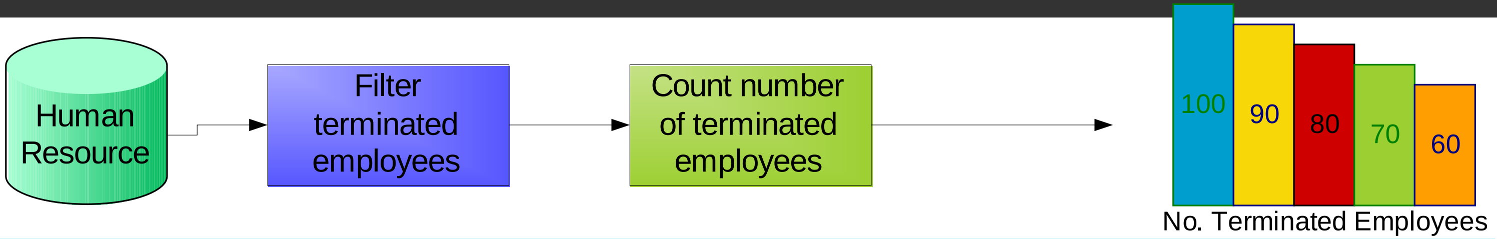

AntiVirus
Count number of virus events where infection date > signature update date
100
90
80
70
60
No. Virus Events Occurred Before Signature Update

Example – What a manager might want to know

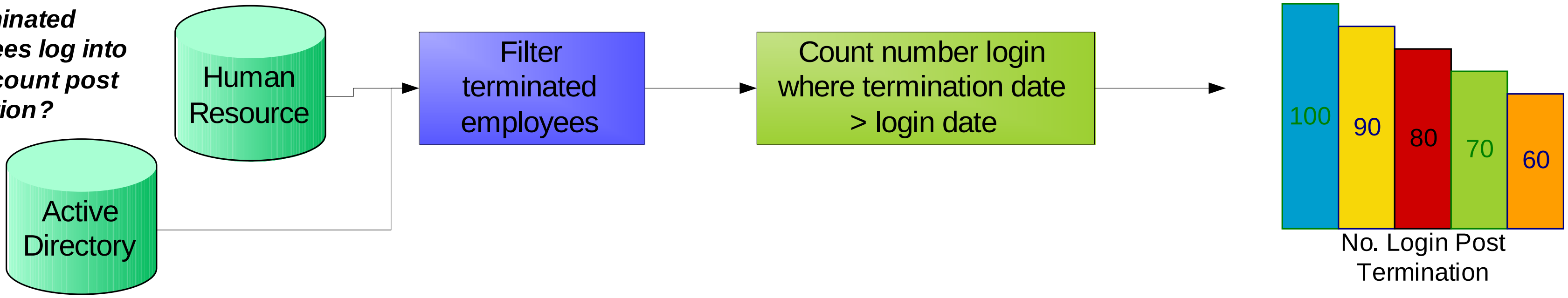
- How many terminated employees were there?
- Did terminated employees log into their account post termination?
- How soon after termination where their accounts disabled?
- Was there a lot of data transferred prior to or post termination?

Example – How we go about getting this information

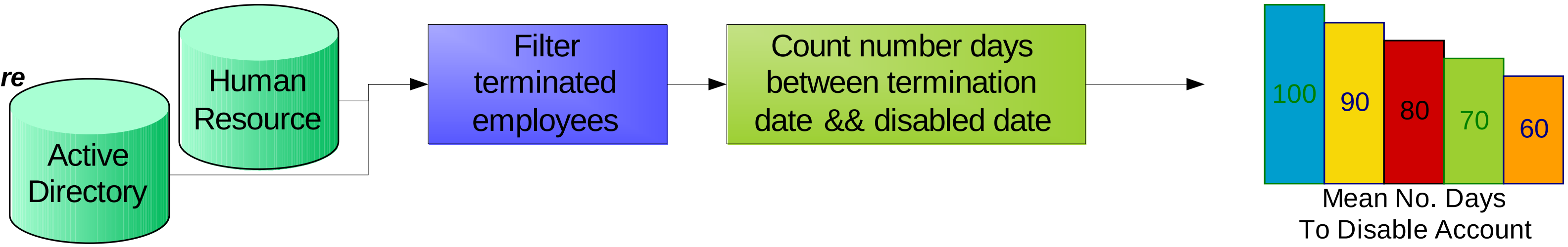
How many terminated employees?


Human Resource
Filter terminated employees
Count number of terminated employees
100
90
80
70
60
No. Terminated Employees

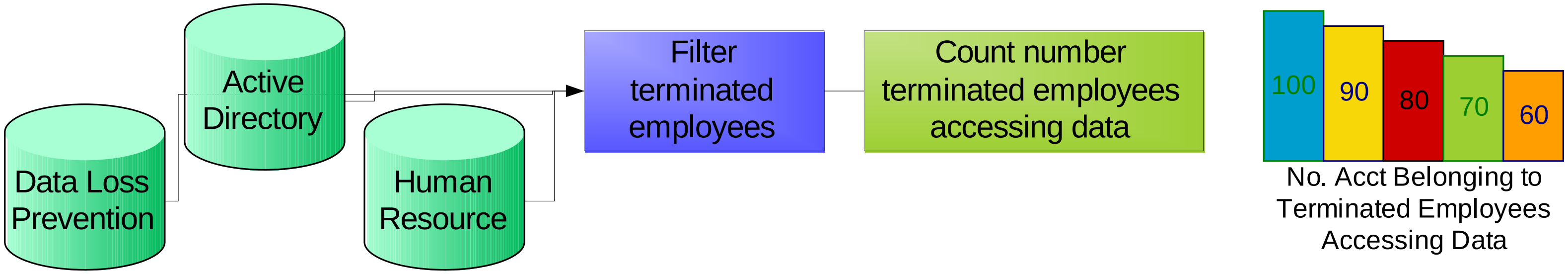
Did terminated employees log into their account post termination?


Human Resource
Active Directory
Filter terminated employees
Count number login where termination date > login date
100
90
80
70
60
No. Login Post Termination

How soon after termination where their accounts disabled?

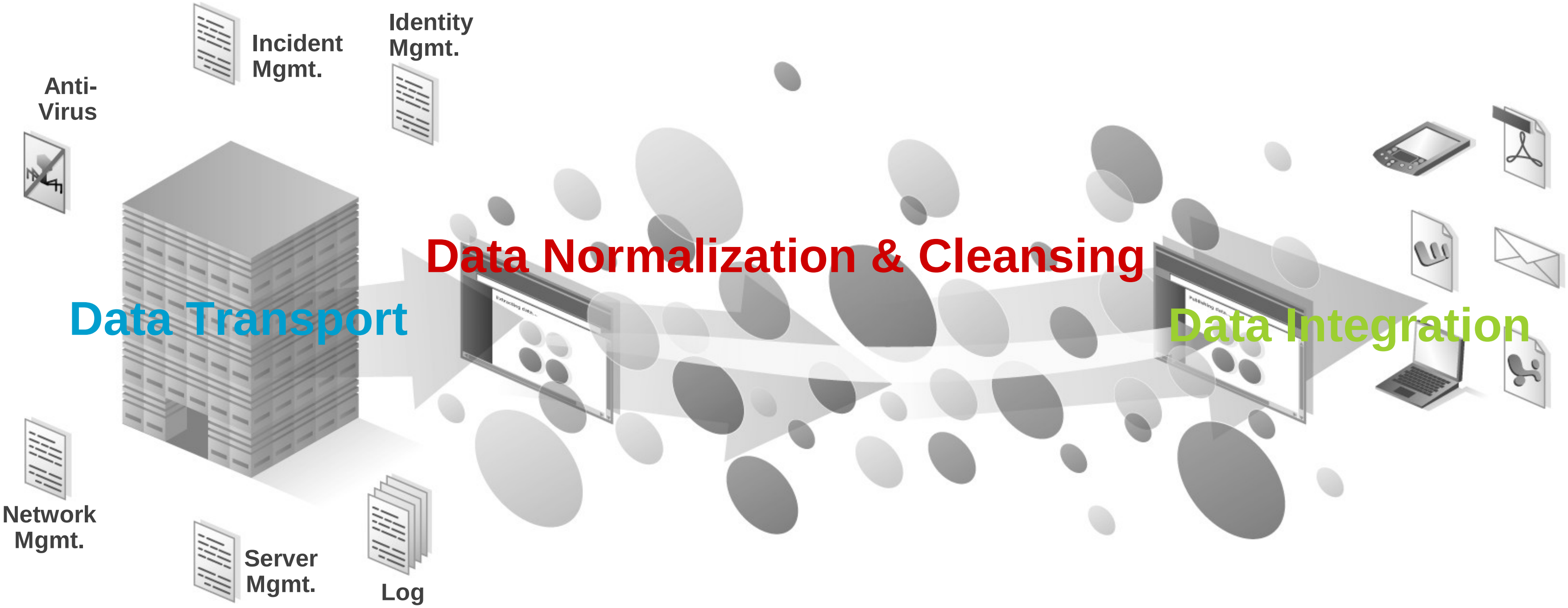

Human Resource
Active Directory
Filter terminated employees
Count number days between termination date && disabled date
100
90
80
70
60
Mean No. Days To Disable Account

Was there a lot of data transferred post termination?

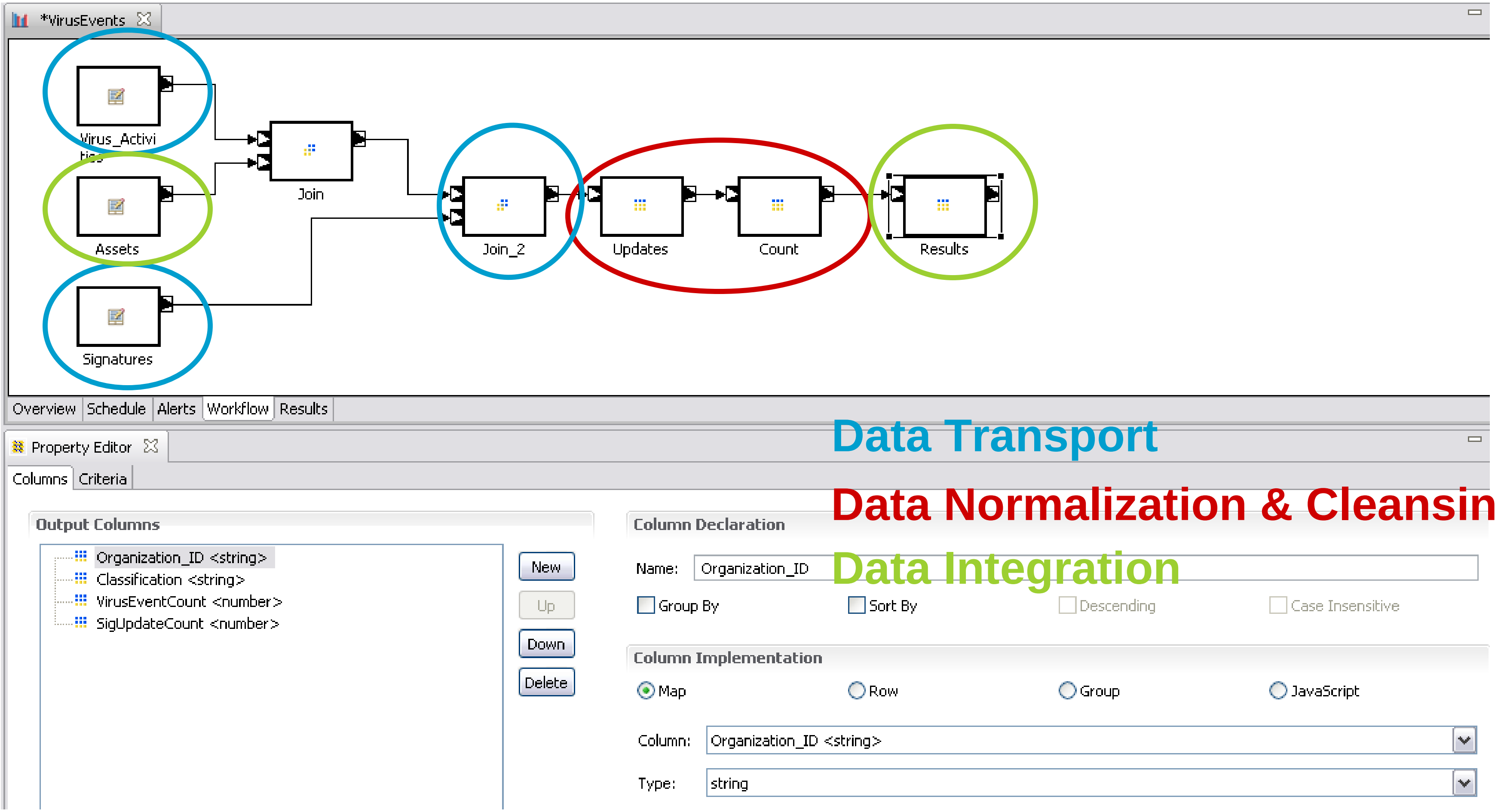

Active Directory
Data Loss Prevention
Human Resource
Filter terminated employees
Count number terminated employees accessing data
100
90
80
70
60
No. Acct Belonging to Terminated Employees Accessing Data

What is a metrics mashup?

- Integration of complementary elements from multiple sources



Performing a metrics mashup



Output Columns

- Organization_ID <string>
- Classification <string>
- VirusEventCount <number>
- SigUpdateCount <number>

Column Declaration

Name: Organization_ID

☐ Group By ☐ Sort By ☐ Descending ☐ Case Insensitive

Column Implementation

● Map ○ Row ○ Group ○ JavaScript

Column: Organization_ID <string>

Type: string

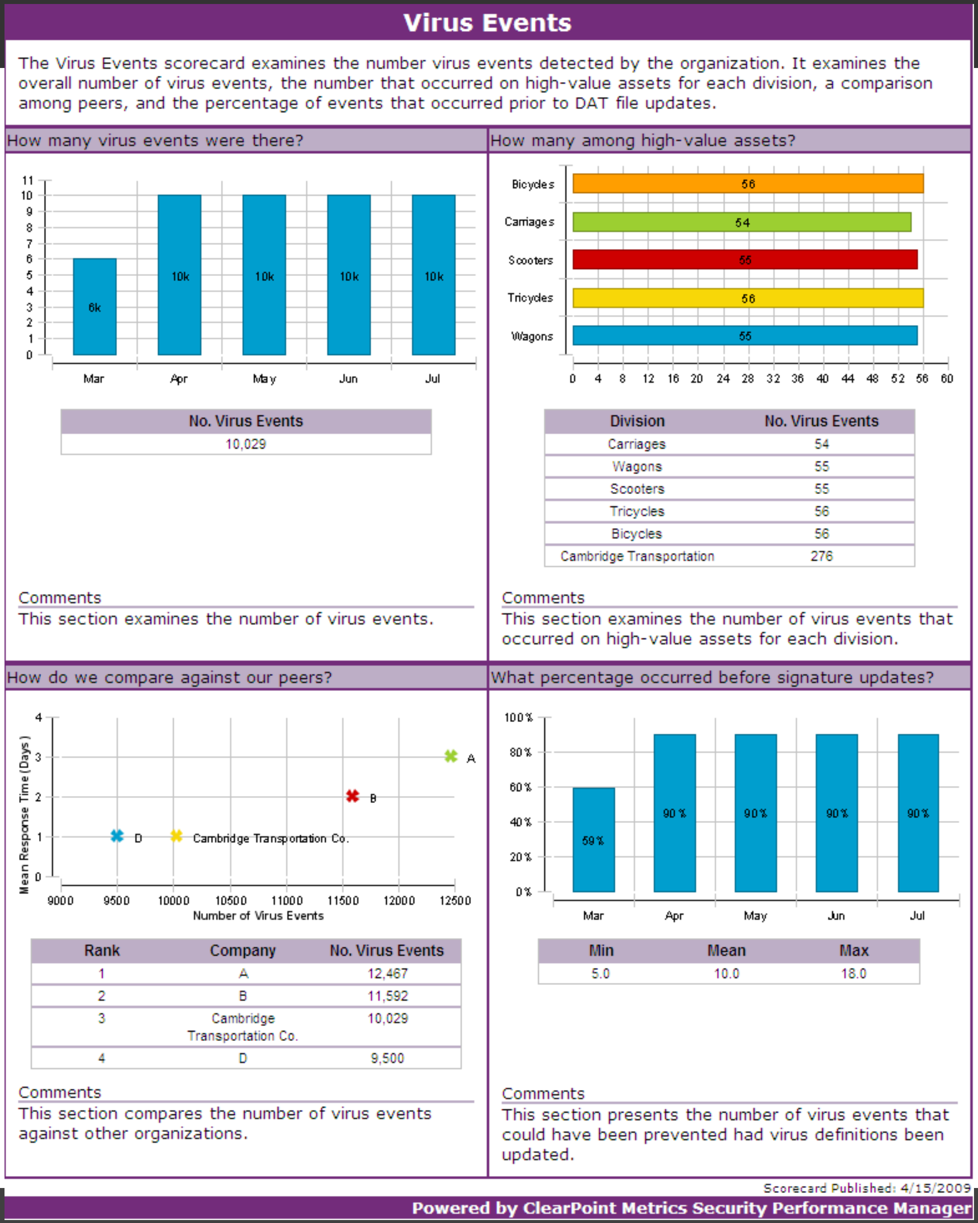
Data Transport

Data Normalization & Cleansing

Data Integration

Results of a metrics mashup

- Provide new and interesting analysis of data
  - Single, integrated view of data from complementary products
  - Enrich data with dimensions (organization, asset classification, etc)
  - Show relationship among products



Virus Events

The Virus Events scorecard examines the number virus events detected by the organization. It examines the overall number of virus events, the number that occurred on high-value assets for each division, a comparison among peers, and the percentage of events that occurred prior to DAT file updates.

How many virus events were there?

No. Virus Events
10,029

Comments

This section examines the number of virus events.

How many among high-value assets?

Division	No. Virus Events
Carriages	54
Wagons	55
Scooters	55
Tricycles	56
Bicycles	56
Cambridge Transportation	276

Comments

This section examines the number of virus events that occurred on high-value assets for each division.

How do we compare against our peers?

Rank	Company	No. Virus Events
1	A	12,467
2	B	11,592
3	Cambridge Transportation Co.	10,029
4	D	9,500

Comments

This section compares the number of virus events against other organizations.

What percentage occurred before signature updates?

Min	Mean	Max
5.0	10.0	18.0

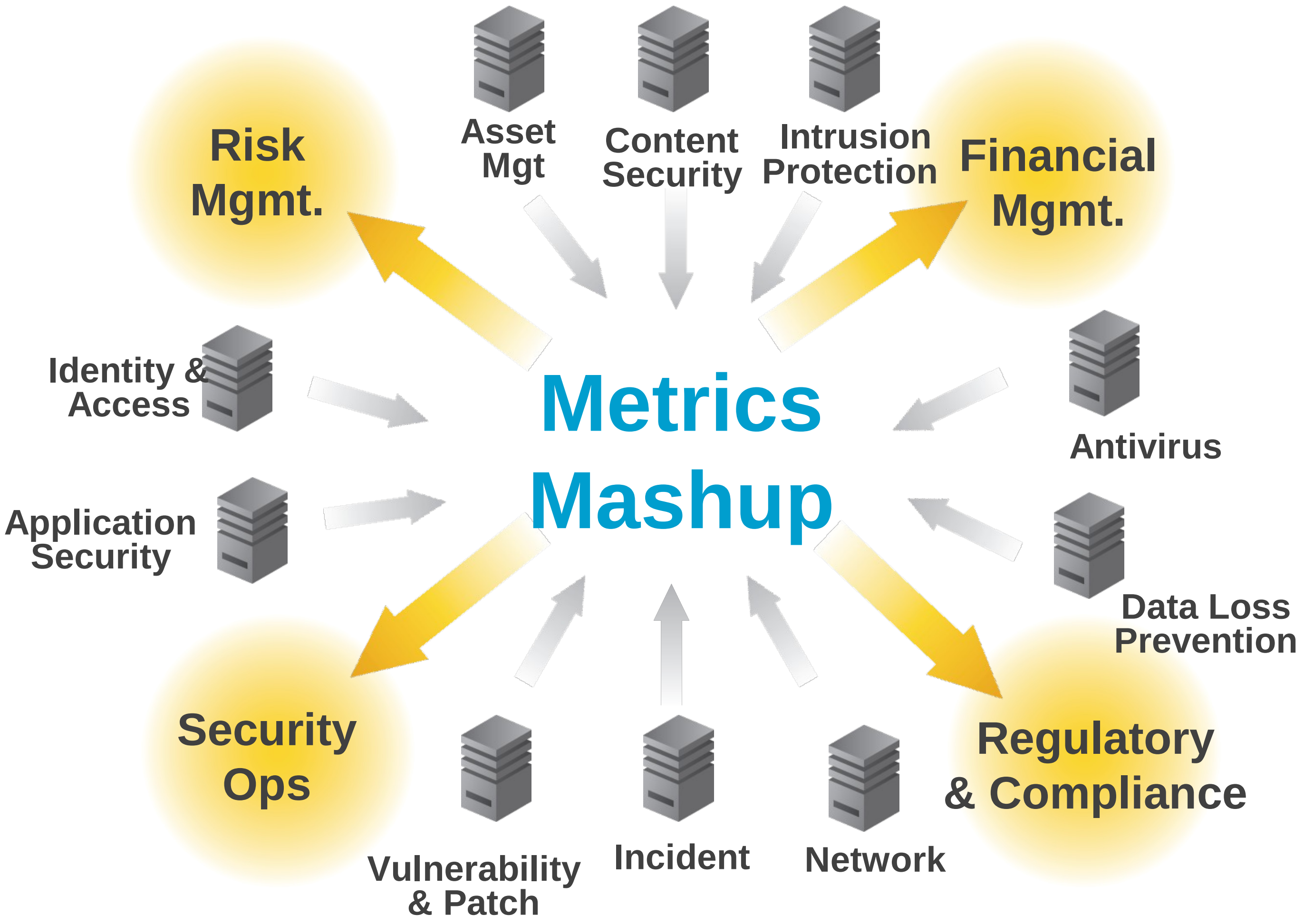
Comments

This section presents the number of virus events that could have been prevented had virus definitions been updated.

Scorecard Published: 4/15/2009

Powered by ClearPoint Metrics Security Performance Manager

Summary


Risk Mgmt.
Asset Mgt
Content Security
Intrusion Protection
Financial Mgmt.
Identity & Access
Metrics Mashup
Antivirus
Application Security
Data Loss Prevention
Security Ops
Regulatory & Compliance
Vulnerability & Patch
Incident
Network

Questions

- Lilian Wang

  lwang@clearpointmetrics.com

References

Caldwell, Matthew. “The Importance of Event Correlation for Effective Security Management.” **Information System Control Journal**. Volume 6. 2002.

Clarkin, Larry and Josh Holmes. “Enterprise Mashups”. The Architecture Journal. http://msdn.microsoft.com/en-us/architecture/bb906060.aspx.

Jansen, Wayne. NIST IR-7564. “Directions in Security Metrics Research.” March 2009.