n-ORM™ Technical Presentation

Phillipe Evrard

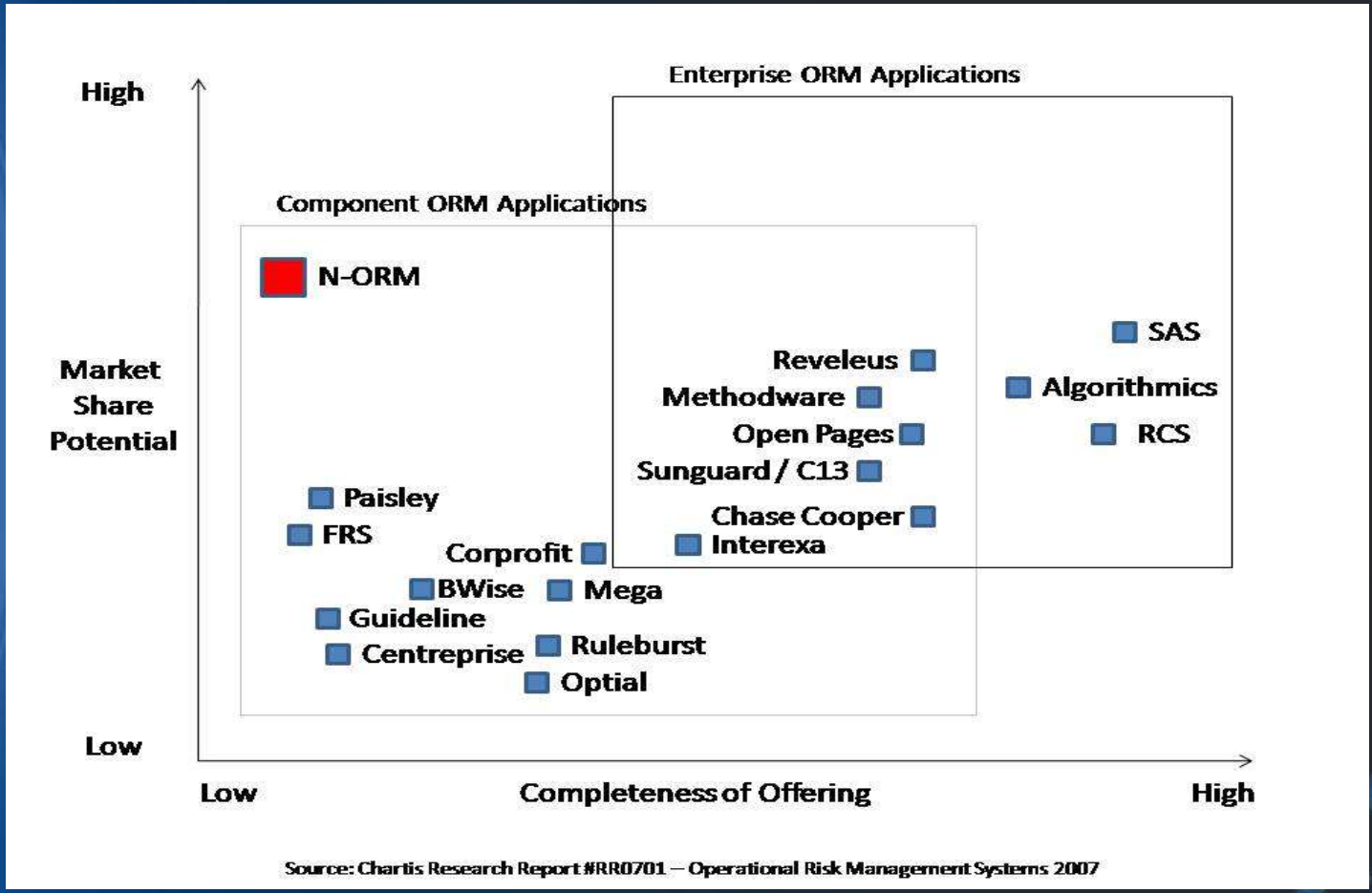
12th March 2009

Risk Management Systems Trends

3 types of players in the market:

- largescale organisations such as Oracle ; SAP ; IBM with add-ons for their ERM and other platforms
- middle market players, such as SAS & Algorithmics
- small players targeting niche markets, such as Popkin; Amelia; Paisley; Coreprofit, etc
- products aimed at either internal usage and controls and external usage for audit and compliance
- activity coverage ranges across the board- from treasury to credit, to political to COBIT

Overall Landscape for Risk Management Applications



Source: Chartis Research Report #RR0701 – Operational Risk Management Systems 2007

What is n-ORM™?

- n-ORM comprises 2 (globally patented) elements;

  a) a traffic collector (back-end)

  b) a system that quantifies the value at risk arising from connecting a corporate network to the internet (front-end)

- It is a compliance tool for Basel II / SOX / Solvency II / Other regulations

- A risk assessment tool as part of an overall risk management methodology

- A means of creating a sectoral loss database

- The methodology to enable underwriting of these risks

What is nOpVaR™?

- The output from n-ORM labelled network operational value at risk (nOpVaR ™).
- Derived from data + algorithmic models within the n-ORM / data capture systems
- Company-specific/unit-specific configured output derived from a combination of automated internal /external data and manually input data
- A monetary value to be used within the overall risk assessment program of an organization.

Current Product/Service Offering

- Complete system
- Volume pricing licensing for 'process manager' element
- Consultancy based upon initial installation, configuration and training
- Subsequent consultancy based upon third party validation of VaR attributed
- System has audit/control report functionality for regulatory compliance
- Historical data analysis for accurate assessment and valuation of risk

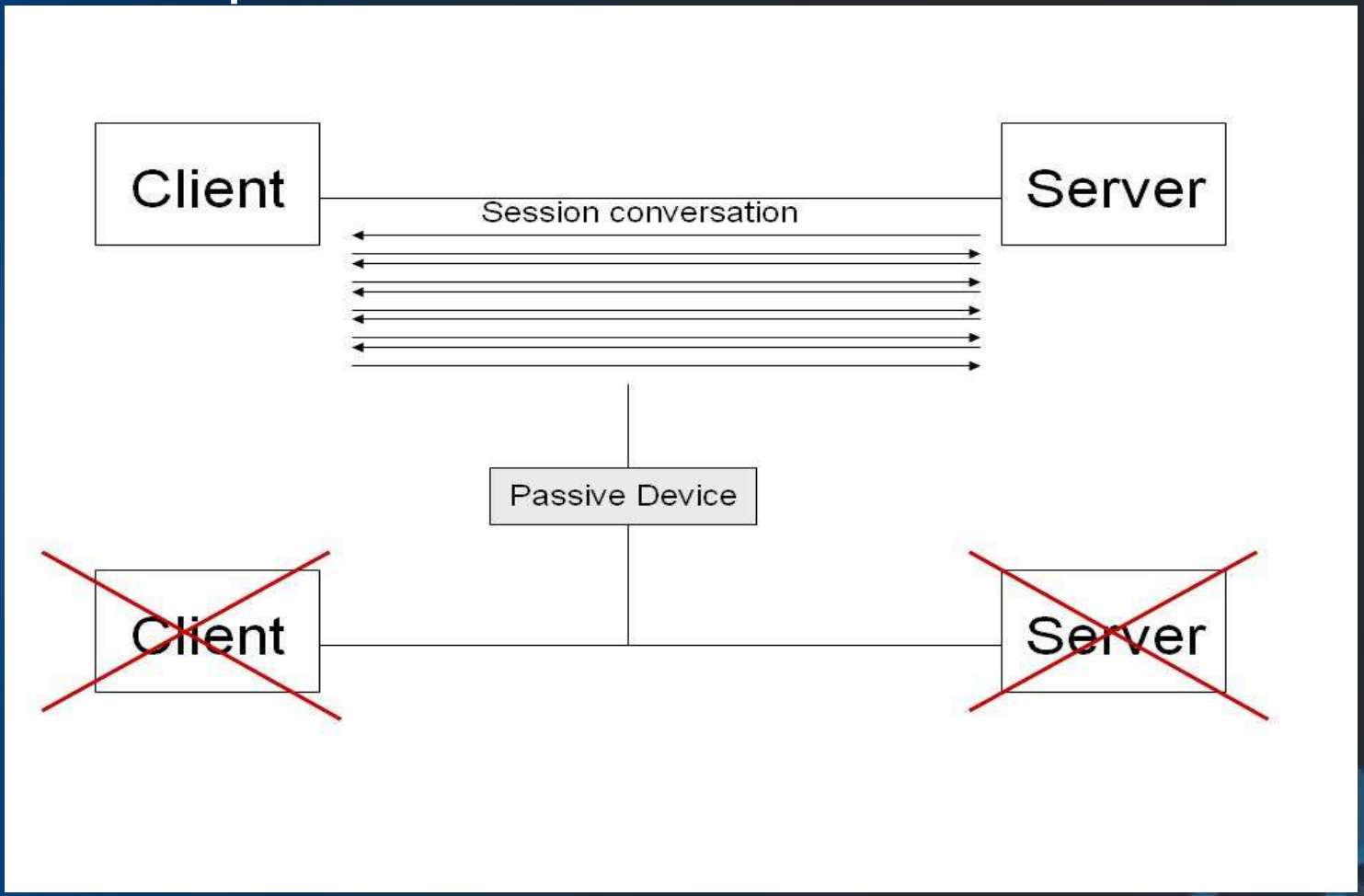
Current Modules / Options

- Full version including front & back-ends; dongle to unlock the limitations on the front end
- Trial version with limited parameters and time-scales
- Stand-alone process manager – multiple process manager modules may be imported to arrive at an aggregated total *VaR*
- Language support. Currently English; Spanish; Arabic

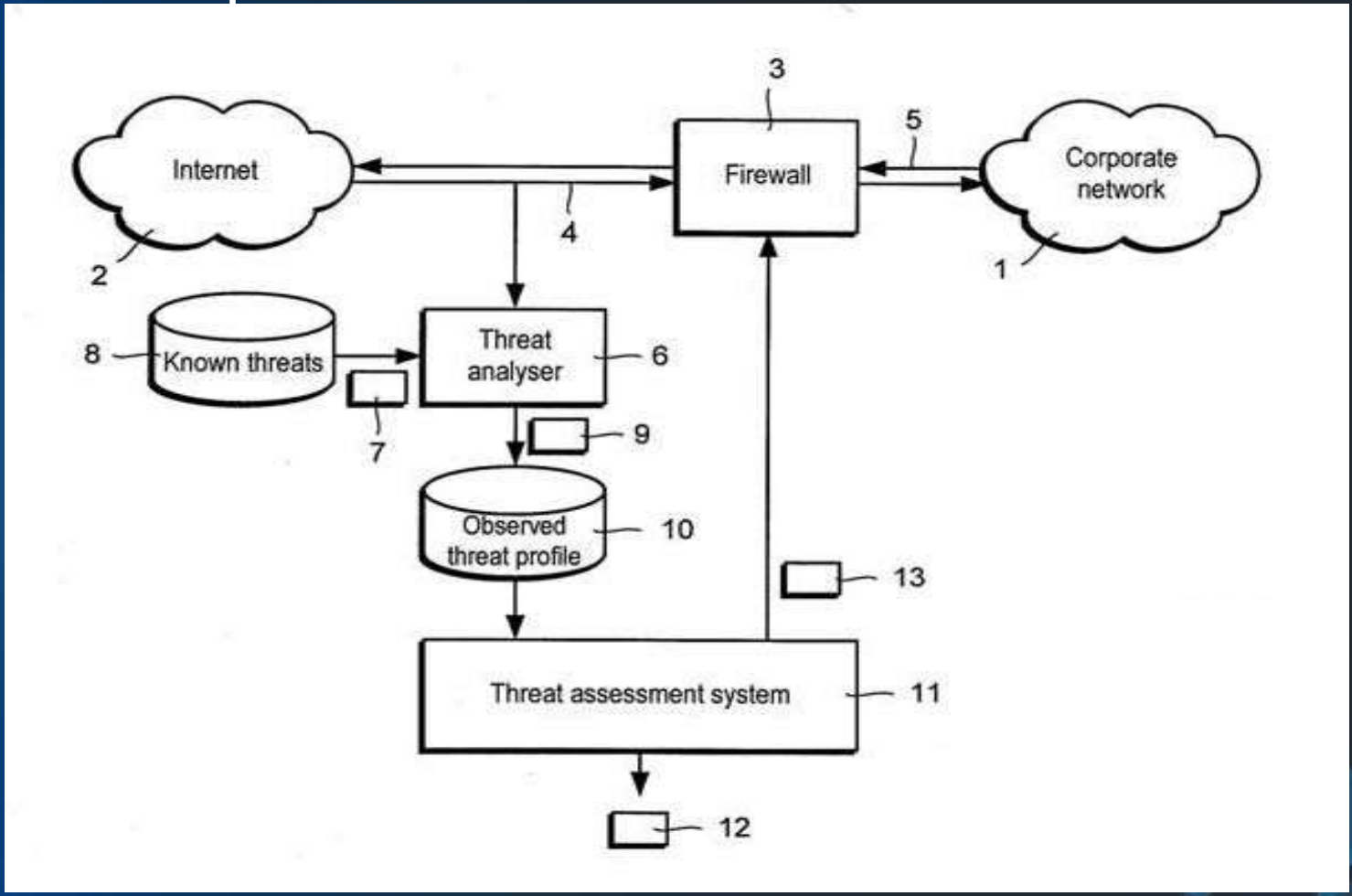
Future Product/Service Offering Additions

- Risk coverage (insurance / risk financing) based upon system VaR output
- Measurement against sectoral loss database (subscription model as per Willis power sector Db)
- Multiple measurement models as optional risk management tools (option to use most appropriate for internal requirements versus reg. compliance
- Varying types of coverage taking multiple inputs (system and organisation-specific)

Basic Copy Model



Installation Positioning



System (2)

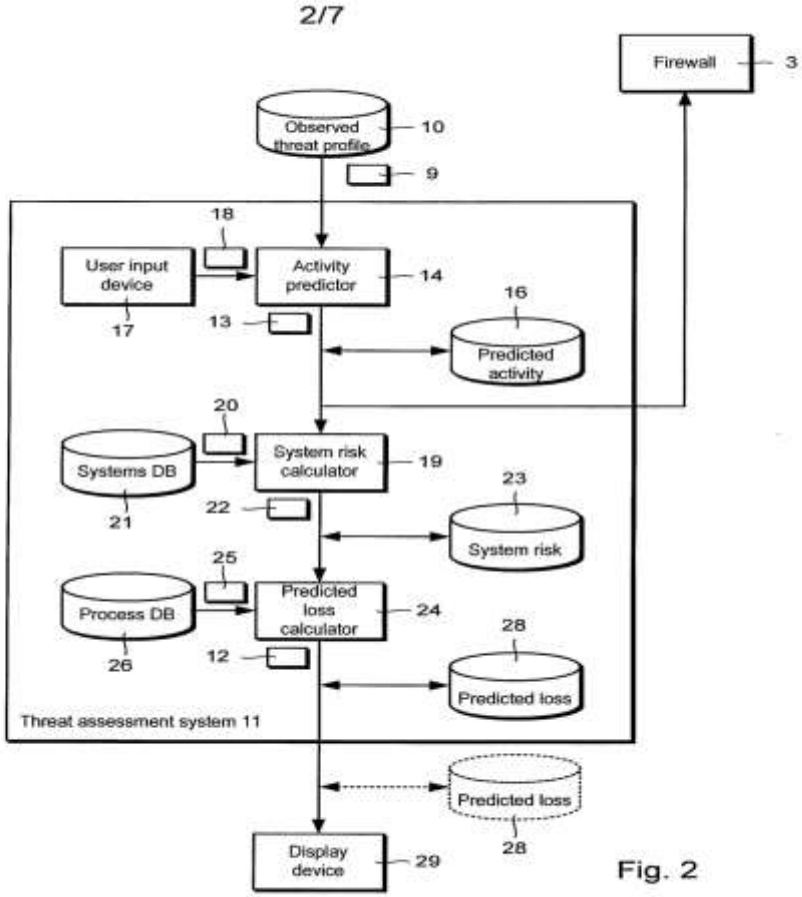


Fig. 2

System (3)

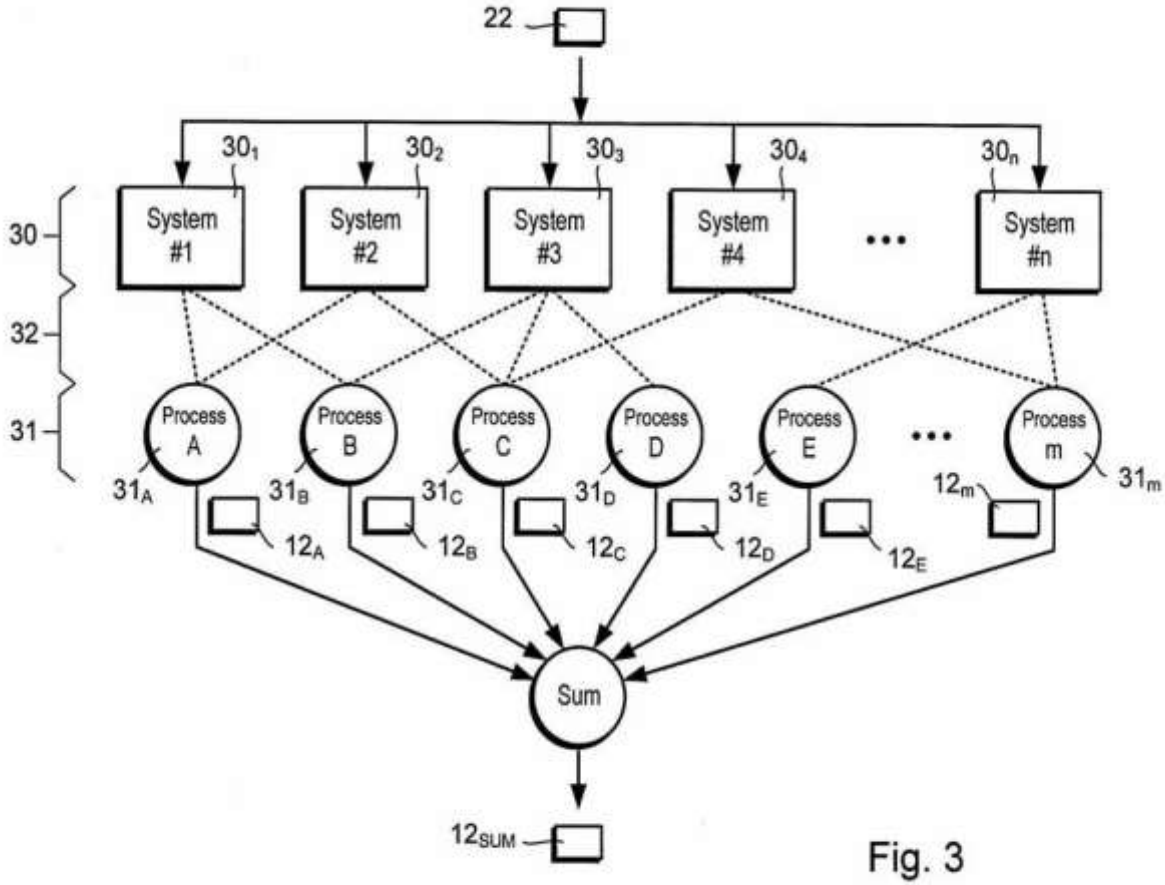


Fig. 3

XML Threat Data

- <Crimson Version="1">–
- <ObservedThreats ObservationStart="2008-02-25T00:00:00" ObservationEnd="2008-03-03T00:00:00">

- <Threat ID="DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">
- <Observation Day="Monday" From="00:00:00" To="00:59:59" Count="52"/>
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>

- <Threat ID="WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">
- <Observation Day="Monday" From="00:00:00" To="00:59:59" Count="247"/>
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>
- <Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>

What Does theThreat Data Mean?

- <Crimson Version="1">–
- <ObservedThreats ObservationStart="***2008-02-25***T00:00:00" ObservationEnd="***2008-03-03***T00:00:00">

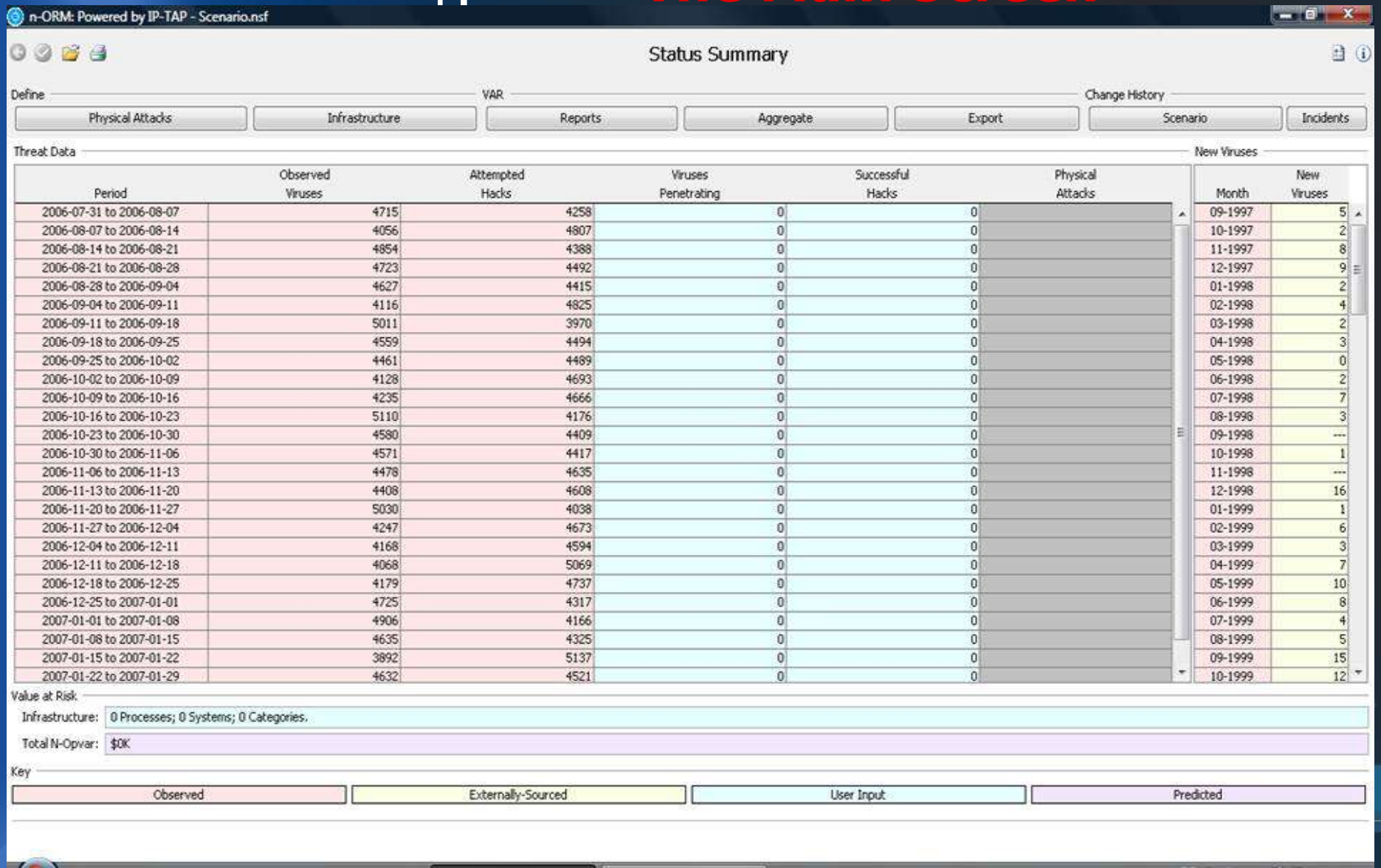
- <Threat ID="***DOS MSDTC attempt" Category="Indiscriminate" Target="Unknown" SeverityScore="7">***
- <Observation Day="Monday" From="00:00:00" To="00:59:59" ***Count="52"/>***
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="32"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="56"/>

- <Threat ID="***WEB-MISC http directory traversal" Category="Indiscriminate" Target="Unknown" SeverityScore="7">***
- <Observation Day="Monday" From="00:00:00" To="00:59:59" ***Count="247"/>***
- <Observation Day="Monday" From="01:00:00" To="01:59:59" Count="152"/>
- <Observation Day="Monday" From="02:00:00" To="02:59:59" Count="266"/>
- <Observation Day="Monday" From="03:00:00" To="03:59:59" Count="437"/>

Main Screen

- Gives a total aggregated risk and value at risk
- Simple to understand
- Audit and compliance focussed
- Reporting and record maintenance of changes create clarity to Supervisors
- Intuitive ease of use requires little training
- Multiple options in the calibration of basic inputs, such as currency, language

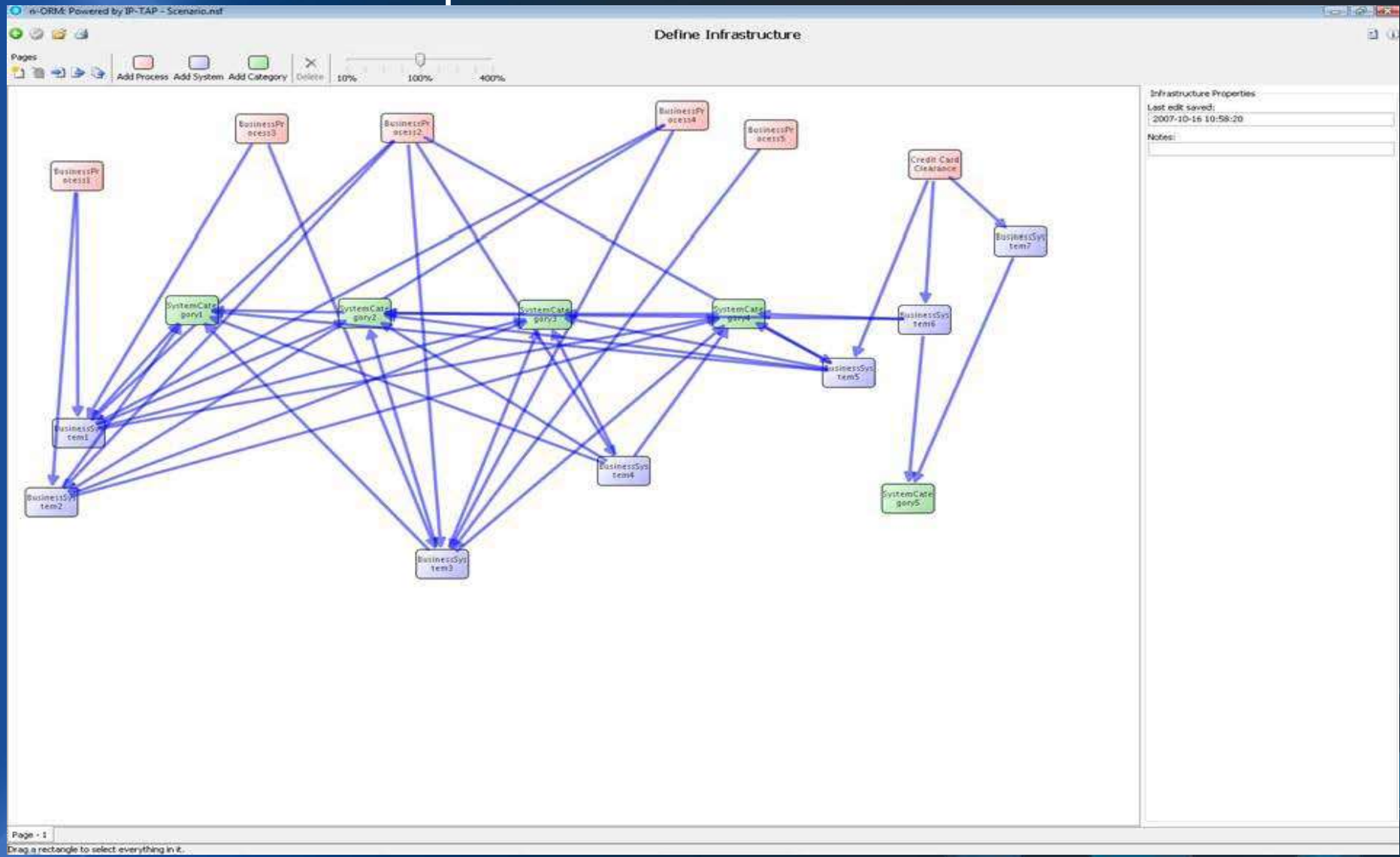
The Main Screen



Process Manager

- Processes, systems and categories are mapped in their relationships by internal personnel
- The output from the process manager is input into the main application
- Multiple instances of process manager can be given to individual workgroups, process managers etc
- Drag and drop functionality reduces training requirements to minutes.

Process Manager



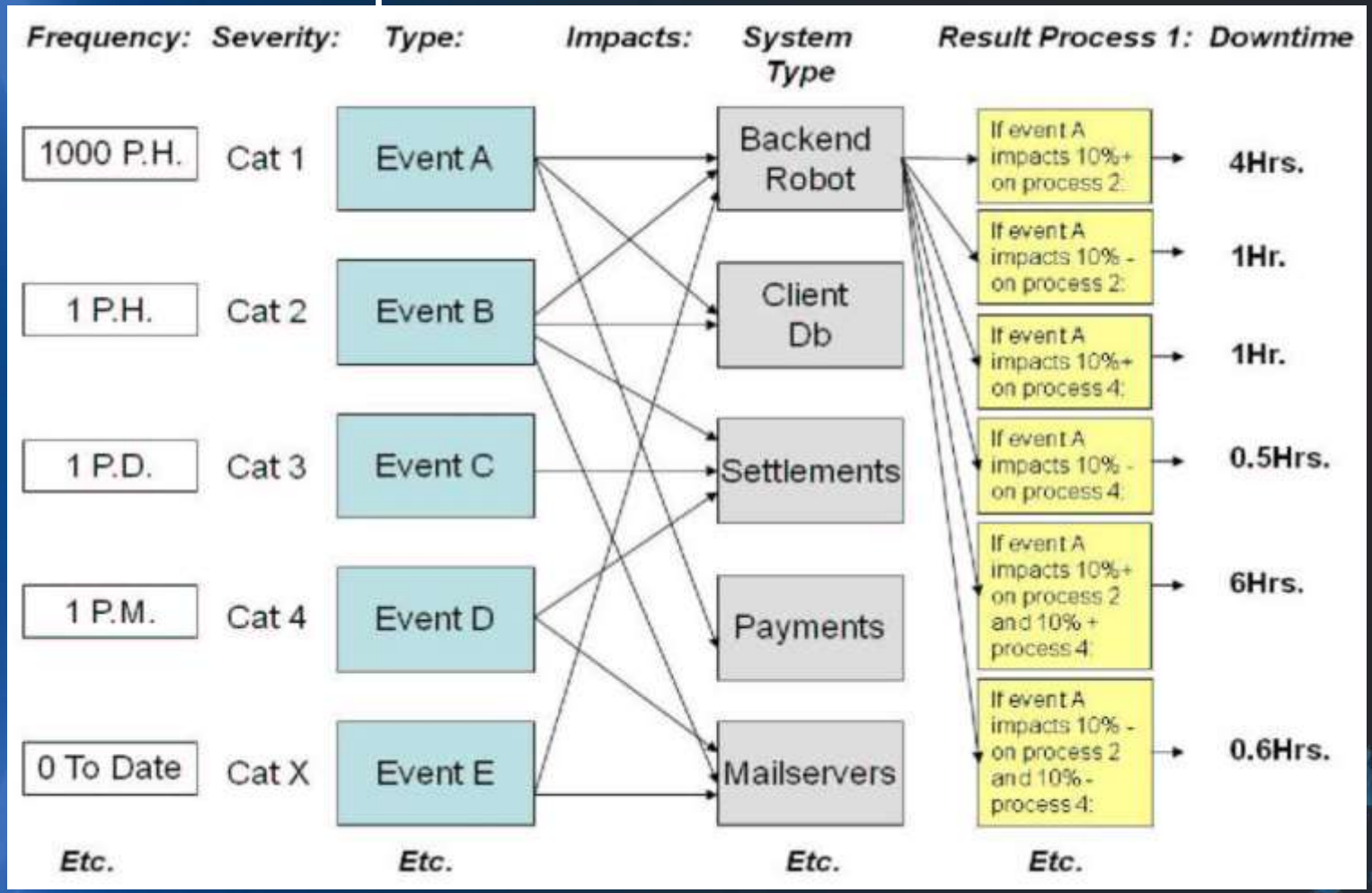
Installation & Licence

- Back-end can be installed by internal personnel with network admin experience
- Can be installed by Loughborough personnel
- Can hold a centralized training day for internal personnel
- Can hold company-specific training per location if small number
- Control of use is controlled by Dongle under specific rights and obligations

Support Structure

- Product support via – NSC (front end) + LUEL (backend)
- Anticipate few requirements for support
- Debugging already undertaken with test site (1.25 years)
- Non-critical / non-real-time system
- Data confidentiality by all parties (only patterns IN the data, NOT viewable data content)
- NSC – military intelligence background i.e. high degree of confidentiality

Overview (1)


Frequency:
Severity:
Type:
Impacts:
System Type
Result Process 1:
Downtime
1000 P.H.
Cat 1
Event A
Backend Robot
If event A impacts 10%+ on process 2:
4Hrs.
1 P.H.
Cat 2
Event B
Client Db
If event A impacts 10% - on process 2:
1Hr.
1 P.D.
Cat 3
Event C
Settlements
If event A impacts 10%+ on process 4:
1Hr.
1 P.M.
Cat 4
Event D
Payments
If event A impacts 10% - on process 4:
0.5Hrs.
0 To Date
Cat X
Event E
Mailservers
If event A impacts 10%+ on process 2 and 10% + process 4:
6Hrs.
If event A impacts 10% - on process 2 and 10% - process 4:
0.6Hrs.
Etc.
Etc.
Etc.
Etc.

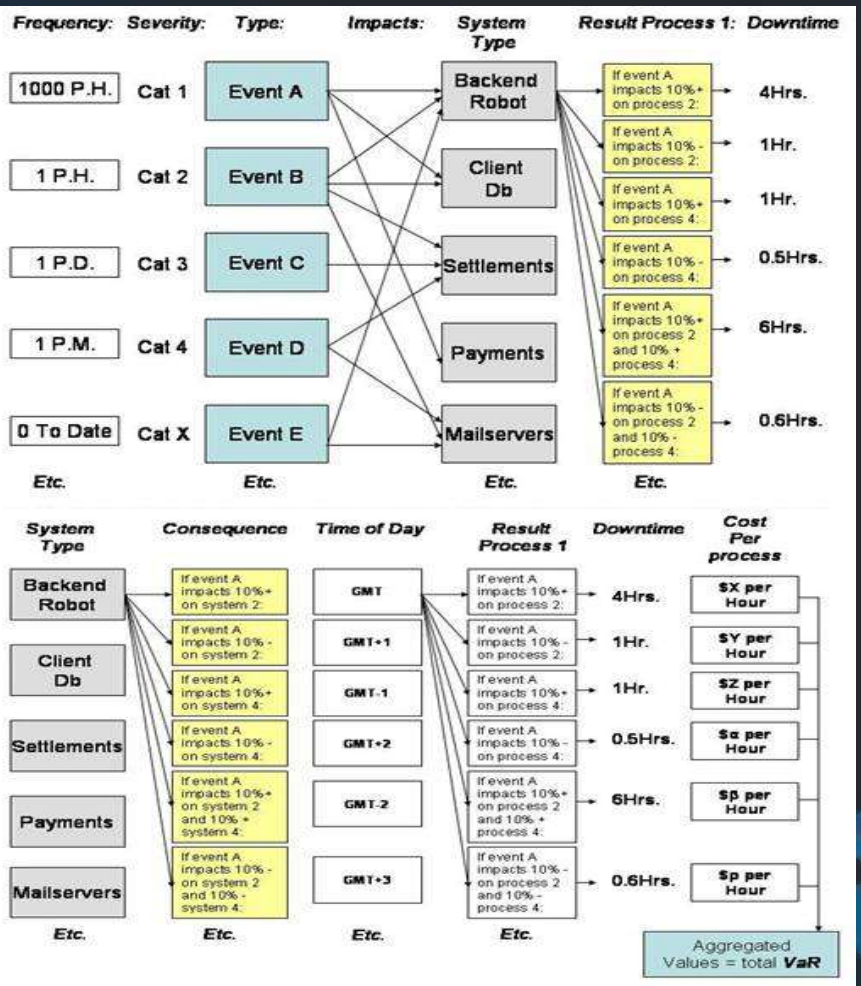
Overview (2)

Data from CVE Db

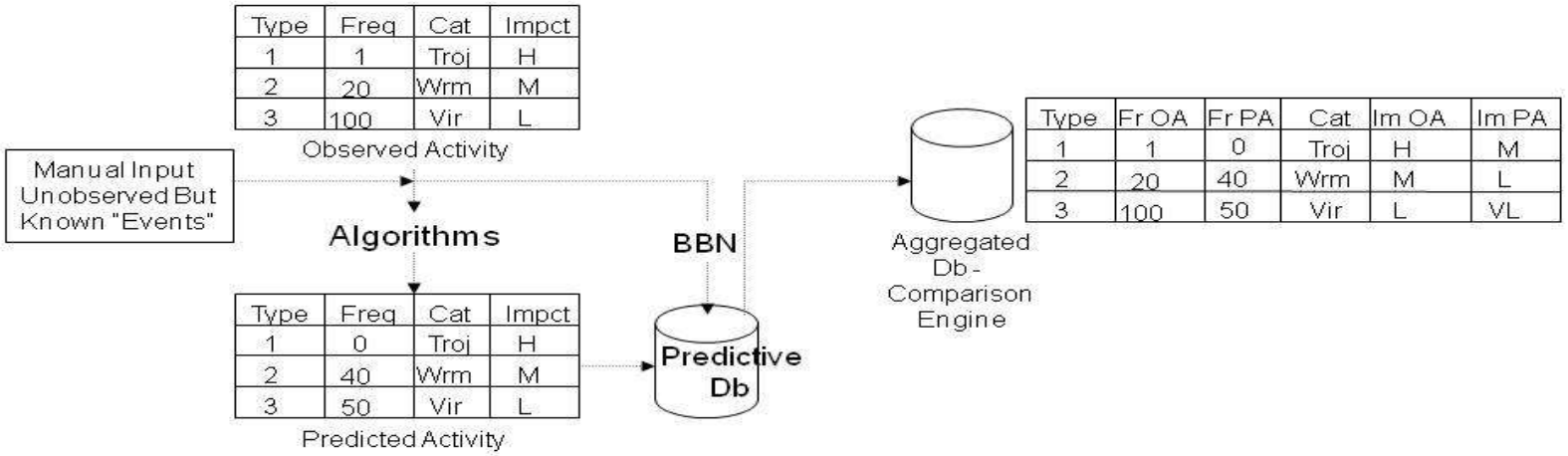
Type	Fr OA	Fr PA	Cat	Im OA	Im PA
1	1	0	Troj	H	M
2	20	40	Wrm	M	L
3	100	50	Vir	L	VL

Type	Fr OA	Fr PA	Cat	Im OA	Im PA
1	23	0	Troj	H	M
2	30	30	Wrm	M	L
3	76	10	Vir	L	VL

Data from Predictive Db



Overview (3)



Manually Entered Variables

Event Type	Process No.	Criticality	Process Interdependence	% Dep.	% Mitigation Reduction	Probability of Mitigation	Totals
1	1a	1	1b	50	0	0	
			4c	10	50	2	
			7a	2	5	10	
2	1b	3					
3	2a	1					

The Algorithmic Models

- Investigation undertaken into the most appropriate based upon test data
- Options were: Weighted Linear Extrapolation; Bayesian Networks; Markov Model; Autoregression.
- Selection based upon a simple approach for customers and Supervisors to understand as well as best fit to trial data.
- Autoregression may be implemented with greater volumes of data to test
- Future development will offer optional modelling methods

Next Steps