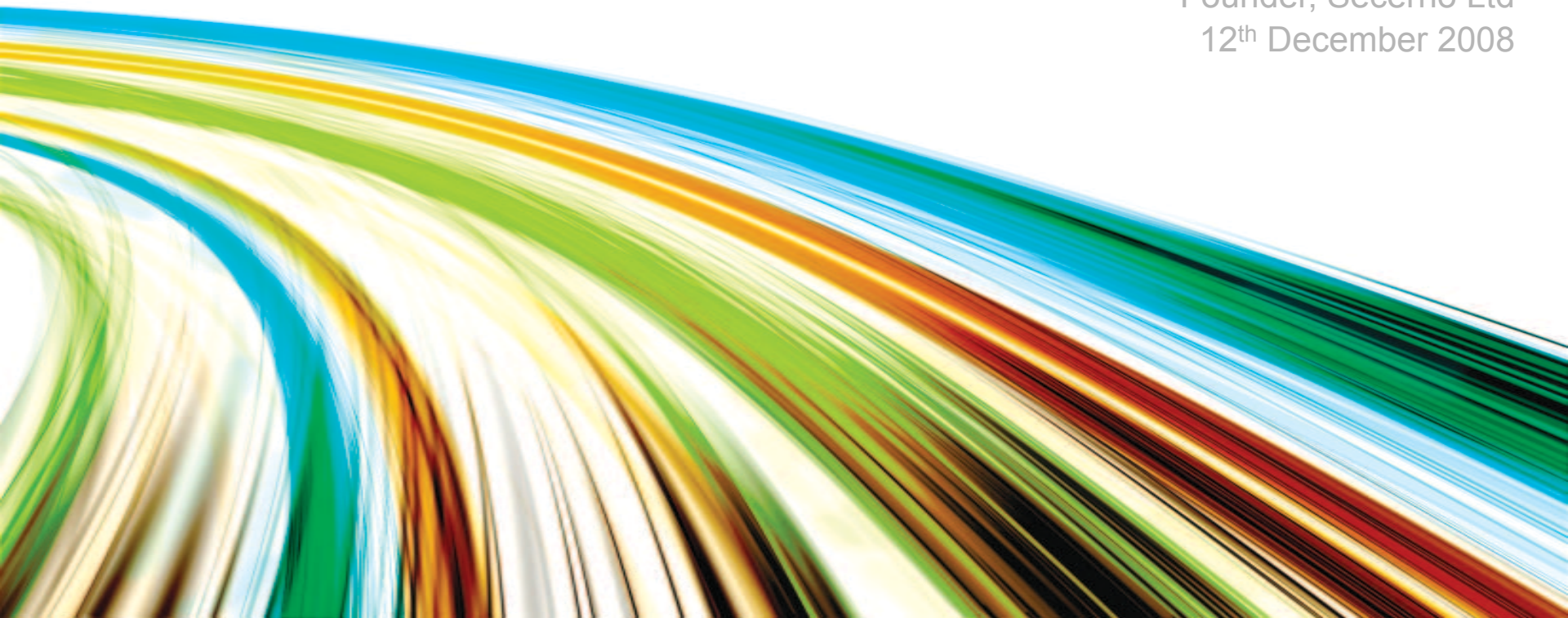
SECERNO

ACSAC 2008

Secured Database – Secured Revenue

Paul Davie
Founder, Secerno Ltd

12th December 2008



Introducing Securno

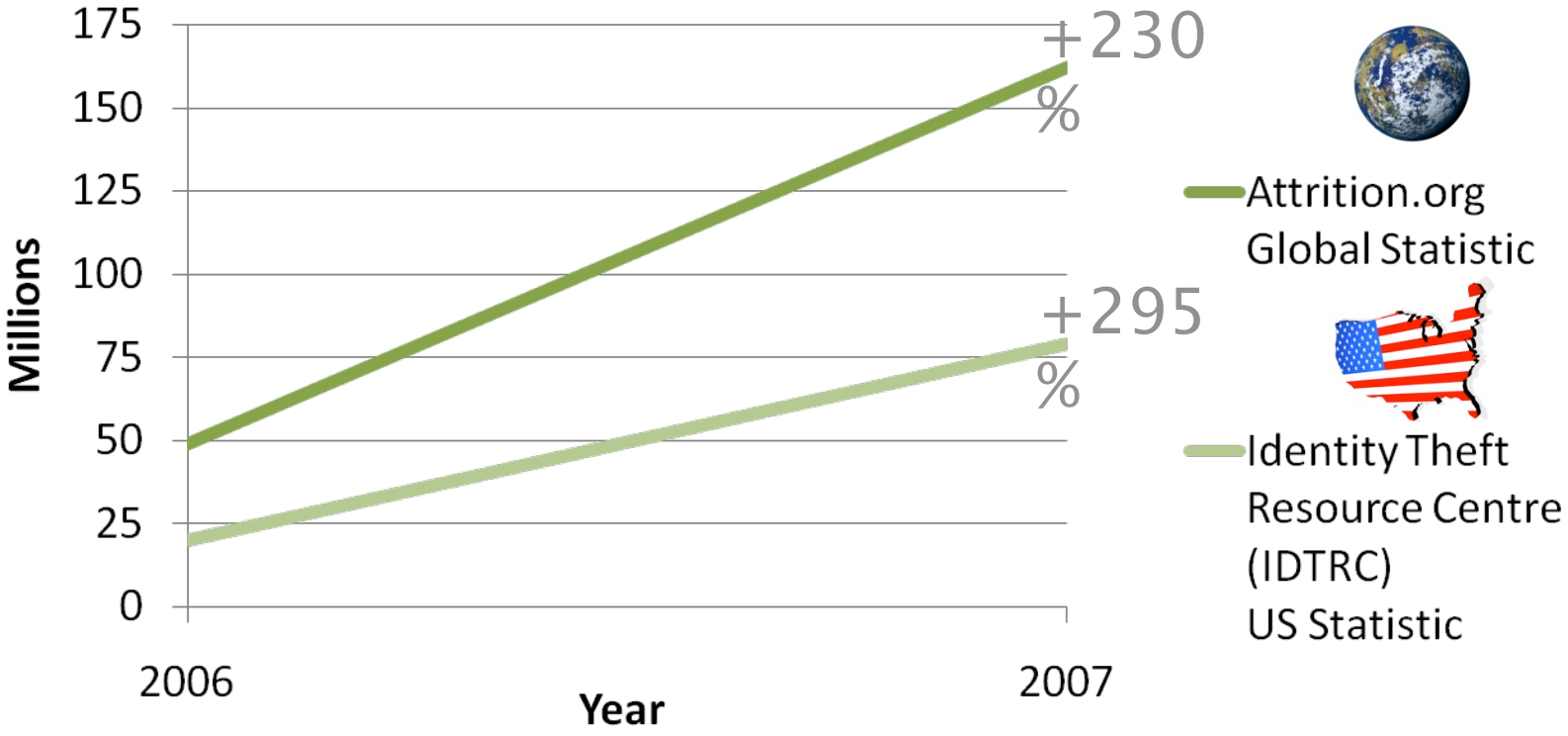
- Current product is the Securno DataWall™ active database security family
  - Deployed as:
    - Hardware appliance
    - Virtual appliance (VMware)
- Headquartered in Oxford, United Kingdom
  - North America HQ: Bedminster, NJ
  - SEMEA HQ: Dubai
- Founded 2003
  - Built on breakthrough research at Oxford University
  - Four patents in progress

Introducing Attraction World

- Attraction World Ltd is the UK's leading theme park and attraction ticket specialist, supplying product to most of the UK's leading travel agents and travel brands.

- Attraction World is committed to the highest levels of service and we are proud to have been voted "Best Ticketing Company" at the British Travel Awards 2006 and 2007.

Data Loss is Growing



- In the first 6 months of 2008 there was a 69% increase over the same 2007 period (Source: IDTRC)

The Costs:

- $197 per breached record, $6.3 m average cost per breach (Ponemon Institute)
- Average 10,000 records lost per incident (Attrition.org)

Q3 Cost of a breach

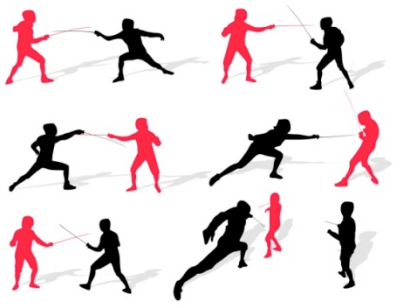
The fallout from a data security breach can be enormous and not just in terms of immediate lost revenue. Some companies never recover because of the lasting damage to their reputation.

Peter Barnsley

Head of IT

The External Threat

- Databases are now closer to the perimeter of the organisation
  - Web-supporting particularly at risk
- SQL injection attacks are still a growing threat
  - 14% of attacks are SQL injection
  - 250% Y-Y growth in SQL injection



- International e-crime has replaced cyber vandalism
  - Focus of crimes is financial gain
  - FBI: Organised data theft is now a bigger criminal industry than the drugs trade
  - Call centre infiltration taking the external threat inside

Protect data not machines: people want to steal

The External Threat

Secerno offered us something different. It would protect the database itself, so we knew that even if a hacker managed to gain access to our network, our database and live transactional server would still be protected.

Peter Barnsley

Head of IT

The Insider Threat to Data

- Driver: control internal use of data
  - 80% of data theft from internal sources *(Forrester)*
- Internal attack sources:
  - 78% from authorised accounts
  - 43% using own ID

  (E-Crime Watch Survey)
- Source of biggest data threats:
  - 42% Employee negligence
  - 33% Broken business processes
  - 15% Malicious employees

  (Ponemon Institute)

- Authentication is no longer sufficient to protect data

"Yes, I know who you are but is this action within corporate policy?"

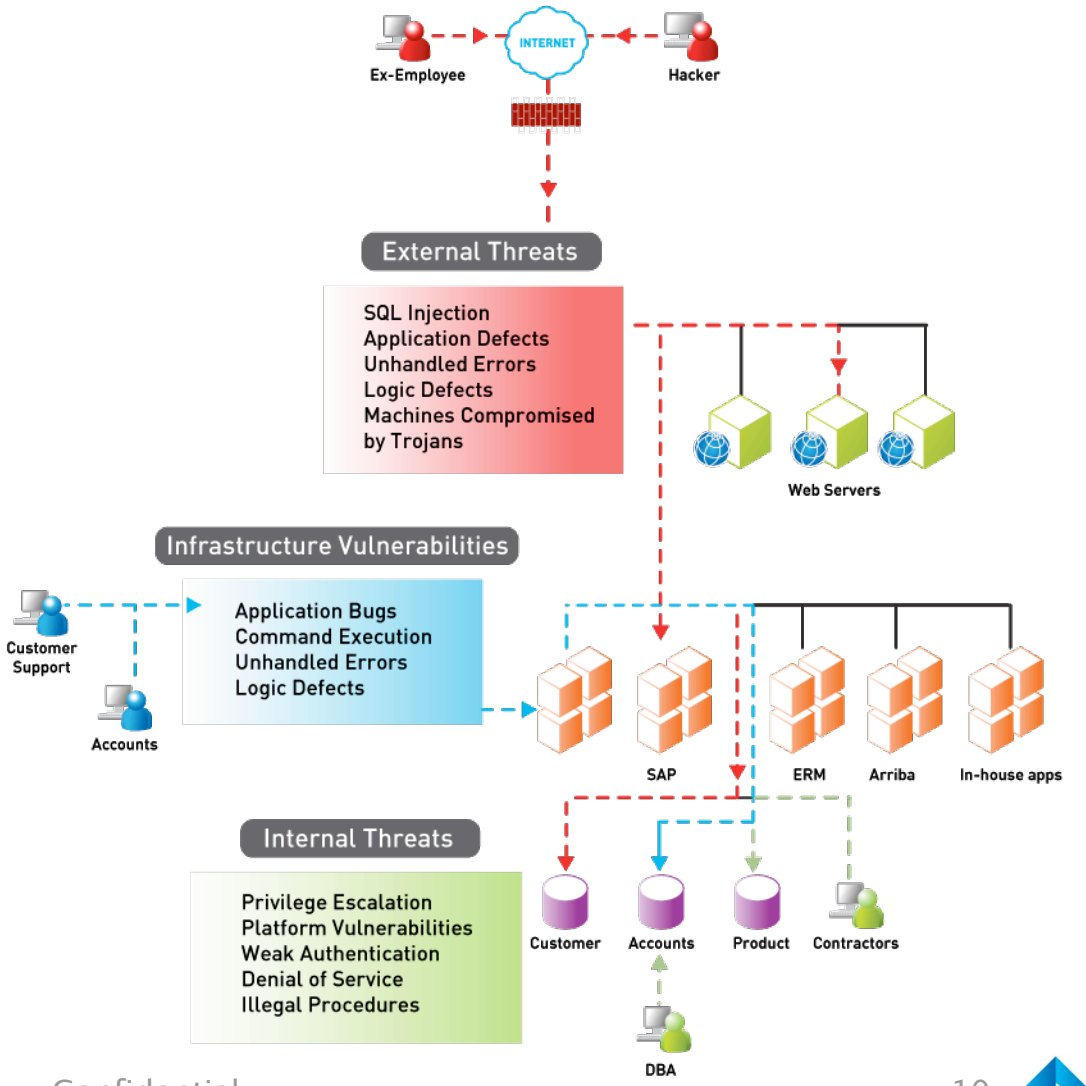
Insider Attacks

When you take on a new employee, you can never be 100% sure of his or her intentions. By having Secerno in place we knew that any insider attack or anomaly regarding database requests would be flagged and we'd be able too protect ourselves.

Peter Barnsley
Head of IT

Data Security Challenges

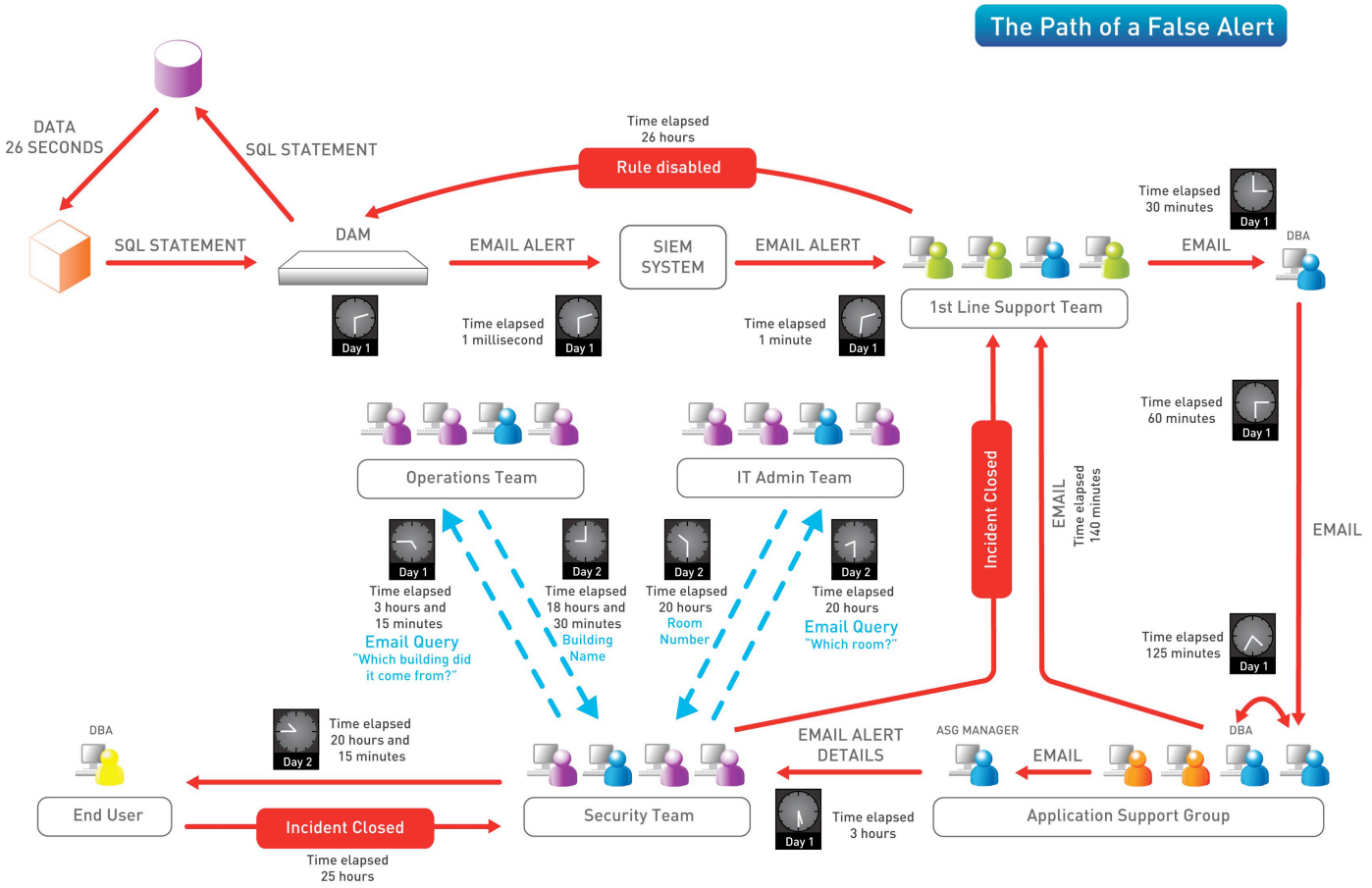
- Mitigate risks of data compromise
  - Internal Threats
  - External Attack
- Improve the security of applications
- Enforce and demonstrate database compliance



Design Requirements: No Signatures

- Signatures can be defeated by:
  - Encoding
  - Structuring
  - Reverse engineering
- Signatures need maintenance and updates
- Signatures cannot support a grammatical language where variations are near-infinite

Design Requirements: No False Positives



Securno DataWall™

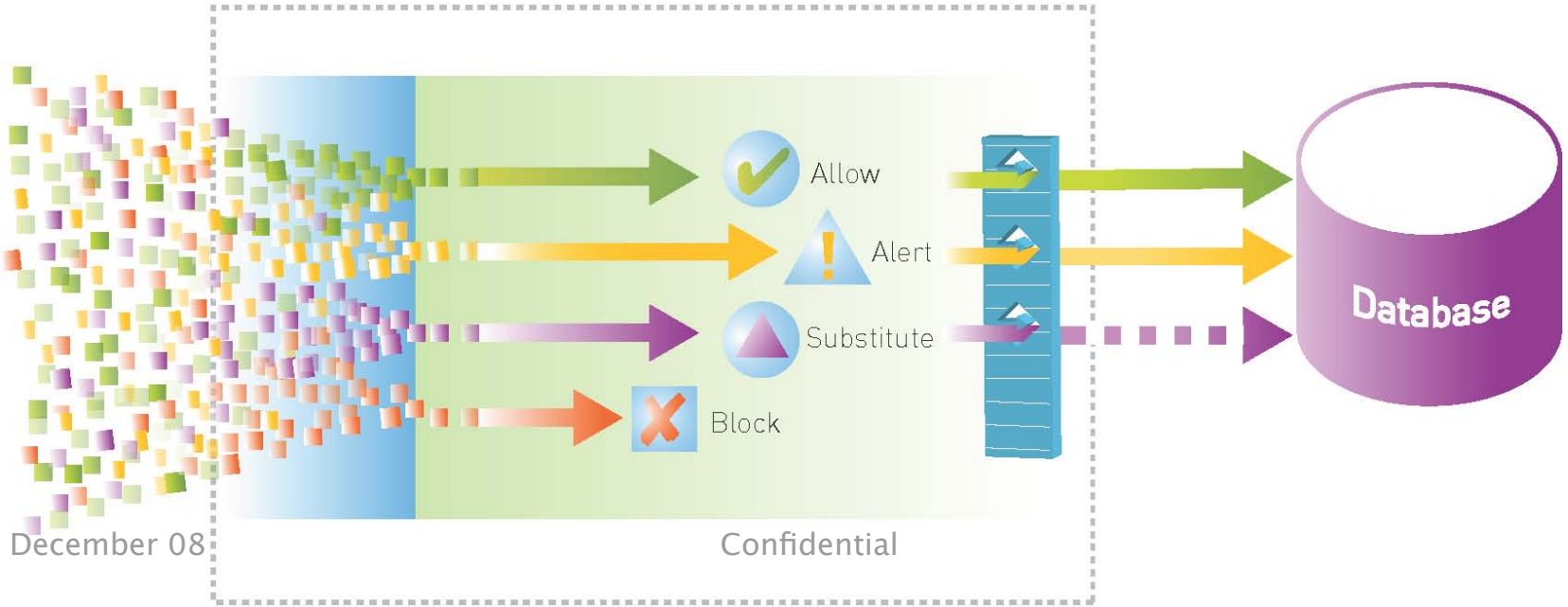
- Securno DataWall™ is fast to deploy and has very low management overheads
  - High performance and scalable solutions
- One solution for many database platforms
- Powered by patent-pending, SynoptiQ technology
  - Millions of individual SQL queries and stored procedures efficiently grouped into clusters of intent
  - Zero policy defects
- Supports best practice in separation of duties
- Does not use native logging (which can have 40%+ performance impact)

Lightest touch solution on the market

- No agents
- No changes to databases
- No signatures
- Fastest policy configuration & maintenance
- Negligible performance impact

SynoptiQ: The Power Behind Secerno DataWall™

- Second generation technology for security solutions
  - Whole statement analysis at the level of the language
  - Manageable display of information
  - Positive security model with zero policy defects
  - Simple policy settings and controls
- Delivers
  - 100% Accuracy
  - Unprecedented Clarity
  - Speed



Accuracy: Speaking the Same Language

- Formal computer grammars form a 4-level hierarchy
  - SQL is Type-2: context-free
  - Regular expressions are Type-3
- Chomsky showed (in 1956!) that Type-2 grammars are too complex to be described accurately by a Type-3 approach
- So:
  - Impossible to *fully* analyse SQL usage using regular expressions
  - *And* ineffective to defend attacks written in SQL using regular expressions

So why do other vendors still use regular expressions?

No Signatures: SynoptiQ in Action

We don't like `union` in this context:

```
SELECT * FROM dvd_stock WHERE [catalog-no] = ''
UNION SELECT [cardNo], [customerId], 0 FROM
[dvd_orders] --' AND [location] =1;
```

False Positives

- Can search for the string union in the hope it will be a keyword unless…
- … there are references to "union bank" etc., or
- … the developer has actually programmed

```
SELECT [lastname] FROM
[boys] UNION SELECT
[lastname] FROM [girls];
```

which will each trigger a false positive

False Negatives

- But what about :
- `uni/* */on`

or :

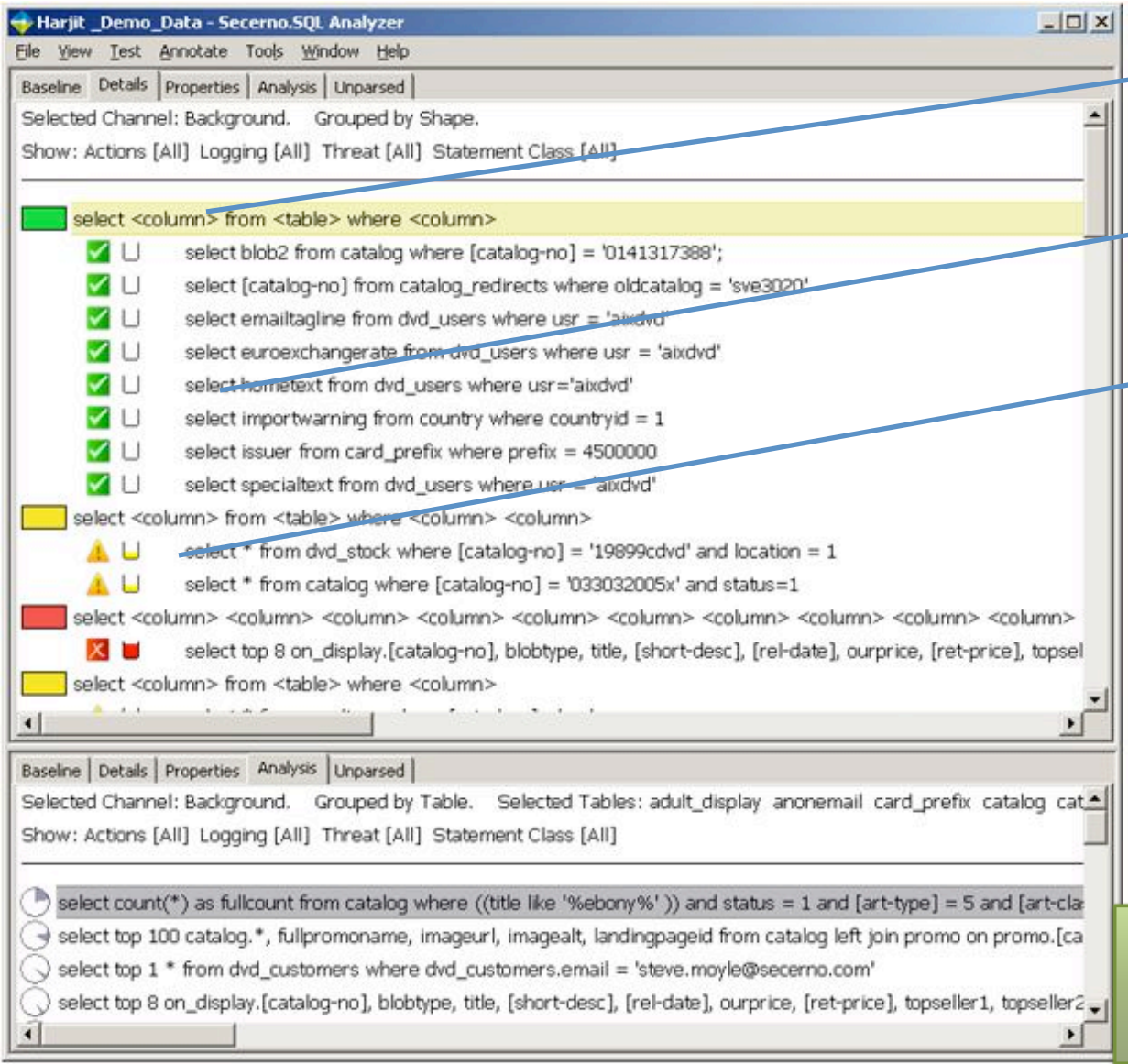
- `u/* */nion`

or :

- `char(117,110,105,111,11 0)`

… which are *semantically* equivalent?

Automatic Analysis of Database Requests; Cluster, Policy & Frequency Display



SynoptiQ clusters by query shape

Queries can come from any table

Queries that are not within the normal distribution are highlighted

Example: NYC Financial organisation

– 57 million SQL statements

Problems with Traditional Query Grouping

- Potentially 100,000s of queries are grouped together
  - Just because they have the same SQL command and Table Name
- This leads to an impossible situation finding the malicious query from the legitimate query
  - Risk of false positives and false negatives
- So traditional solutions have to rely on signatures, because their understanding of what is in a SQL query is incomplete

The Problem

- Inefficient, time consuming policy configuration and maintenance
- False positives (crying wolf)
- Inability to effectively alert, block and substitute

"...so you do all the easy work grouping the queries and leave us to do the hard stuff...."

Financial institution, looking at a traditional solution

SynoptiQ vs. Traditional Comparison

- The same database (2,817,834 queries / day) is efficiently clustered by SynoptiQ

Traditional	SynoptiQ
216 query groups	35 clusters/group
700,000 max group size	72 max cluster/group size

- Traditional grouping methods require signatures to augment poor query analysis, SynoptiQ does not

The Result

- SynoptiQ is >600% more efficient at clustering queries than traditional methods
- Secerno can be deployed in-line with no operational risk or performance impact

SynoptiQ: Summary

- 100% accurate analysis
  - SynoptiQ's analysis of SQL intent is not confused by nested commands, SQL remarks, leading quotes or semi-colons, or highly irregular SQL statements
- 100% accurate positive security model
  - No signatures
- Semantic Clustering™ delivers manageable display of information
  - 600% more efficient than traditional solutions
- Fast policy settings and controls
  - Automatic threat and policy assignment

The Result
- Fast, effective policy setting and maintenance
- Zero policy defects
- Accurate alerting
- Selective blocking and substitution is feasible

Return on Investment

If Secerno prevented an attack that would have cost us 24 hours' worth of data, it would represent a return on investment of 400%. That's not taking into account the cost of lost or corrupted data or repairing a damaged reputation.

Peter Barnsley

Head of IT

Applications

Secerno highlights vulnerabilities and shows us not only where and how we can tighten security, but also where we can optimize the application. The system highlights errors in the application which, once remedied, make the application run smoother and faster.

Peter Barnsley
Head of IT

Audit

We have implemented the actions recommended by Secerno and have reached a level of security that is acceptable to the banks.

Secerno actually helps us win new business because we offer bank-approved security

Peter Barnsley

Head of IT

SECERNO

ACSAC 2008

Secured Database – Secured Revenue

Paul Davie
Founder, Secerno Ltd

12th December 2008