ABSTRACT

BusinessForensics develops solutions for enterprise risk and fraud management. We entered the challenge to develop a generic visualization of worldwide equipment states in time critical scenarios. HeadQuarters, our main product, has earned a ‘good visualization award’.

Keywords: Enterprise investigation and decision support; Event profiling; Visualization; Configuration Management; Risk & Fraud Management.

Index Terms: H.3.4 [Systems and Software]: Enterprise investigation and decision support; H.3.3 [Information search and retrieval]: Complex event profiling.

1 INTRODUCTION

All tools mentioned in this summary are developed by BusinessForensics. HeadQuarters (HQ) is an investigation tool which provides a generic view on objects and the events they generate. Its database has only four important tables: entities, attributes, links and facts. This high abstraction allows HQ to build representations of ‘reality’ behind any business process. HQ is complemented by a profiler, which tries to identify unusual activity in a stream of events. In this case the machines, business units and departments are represented by entities in HQ.

2 ENTITIES

HQ entities are designed to identify, name, date and locate any domain object (machine, department, business unit). Entity details are stored as separate attributes (1:N). Finally, the relationships between entities are stored as links (N:N). Facts are used to link administrative transactions to their corresponding entities (events to machines, orders to customers, transactions to accounts, etc.)

HQ is very strong in visualization, user experience and versatility. So for us, this challenge provided a great opportunity to build a generic view of object states on a world map. The challenge was focused on Google Earth, but we were limited to an ESRI map component, which was already integrated in HQ for finding an address on the map.

3 THE PROFILER

BusinessForensics Profiler didn’t have any problem with the volume (159 million rows) because it’s designed to profile 10K transactions per second. It’s an early warning system for large enterprises, designed to identify unusual changes in real time.

The Profiler has input adapters for incoming data (files, queries and queues), a rule engine and a profile store (MSSQL). The rule engine is using dynamically compiled C# code to transform data, to implement business rules and cache frequently used profiles.

The Profiler creates individual event statistics for all significant objects (IP numbers) in the data and ‘learns’ how they usually operate. It also creates enterprise level statistics, represented by the lower tiles in the engine:

In this case, the profiler identified huge amounts of warnings, alerts, critical and supercritical issues. This high level information had great effect on our approach because it showed a glimpse of what finally happened to the bank.

4 THE MAP

After completing the profiling session, HQ had access to individual machine profiles, original events (facts) and background information (entities for machines, departments, etc.). The original events were updated with geographic coordinates during profiling which saved MSSQL from an ‘expensive’ table join.

So now the only barrier between the facts and the map was a SQL stored procedure accepting a date range, a map extent and a resolution. This stored procedure allowed us to create a dynamic dataset with enough information to draw dots on a map. The dataset was created by grouping warnings, alerts, issues and critical events, summing them up and grouping the totals to XY coordinates. We rounded these coordinates to the nearest integer at a global scale and used full precision when zooming in.
This provided a simple and straightforward way to visualize and fine-tune whatever we wanted to see. We decided to use black dots for static machines (inactive), dark blue for warnings, red for issues, orange for critical matters and yellow for virus alerts. We used variable sizes for the number of machines on a single coordinate. Layers and transparency were used to avoid dots hiding under bigger ones.

We filled the regions on the map using the KML document supplied with the challenge. The ESRI control usually shows the world map and allows you to zoom in on any level of detail, but our screenshots are optimized for the stills used in the video. The world map layer is dimmed using a slider (top of screenshot) which also allows you to dim individual layers. On the left there’s a list of ‘most important issues’. Its content is also defined by the stored procedure, so you can easily adapt this view to your needs.

Clicking on a dot will trigger a select query, which takes you to the entities, attributes, links and facts in HQ. Here you can drill down from any machine to any related configuration item.

5 Visualization results

This challenge has been a great experience for us. It helps us to improve our products, but more important: it helps us to better understand the needs of the professional analyst.

In the following table HQ shows the areas that were considered as anomalies.

There’s an off-line datacenter in the north, which eventually comes active and also gets infected.

There’s a blackout in the east and renders the machines off-line.

Machines under maintenance continue to serve their users.

We missed some workstations working outside business hours due to the high alert count. We modified the system to toggle and tune individual layers.

We noticed that maintenance stopped at precisely 06:00PM - with all these alerts going on - but it was not considered an anomaly. We also identified thousands of infected ATM machines, which triggered our imagination from a forensic point of view.

6 Final state of the Bank of Money

With HQ were able to create a worldwide, configurable view on the Bank of Money’s health. As the Profiler had already predicted in its first run, the Bank of Money would end up with 24 million minor-, 7 million serious-, 1.4 million critical- and 700K of infection events. Here’s how it looks in retrospect