

Subject:	Security Incidents whitepaper
Version:	1.0
Date:	9.1.2008
Author:	Jiří Helešic, Cyber Fox, s.r.o

1. WhitePaper

Security Incidents (SI) is an application designed to file and process all unusual or nonstandard events (security incidents) that may occur in company environment. SI manages complete incident cycle, from the report stage through examination to final enclosure and monitoring of trends.

After installation, it is immediately available through web browser to all allowed users within specified network.

Though client tailored application, its design is very flexible, in order to adequately respond to any process changes in client's company environment.

1.1. Key features

1.1.1. Web user interface without installation

Users can use the system with their web browser, it's not necessary to install anything.

1.1.2. Using of prepared or your types of incidents

There can be more incident types to distinguish recorded situations including variety of fields in each type.

You can use predefined types of incidents, alter them or define new ones with your own fields to fill and search in.

1.1.2.1. General incident for common users

All employees can submit incident on one entry page without detail knowledge of system function, they can simple fill their name, contact (both automatically prefilled from Active Directory) and one text area to describe their problem. Incident is then processed by general incident manager who can convert it to a specific type and assign to specific solving person.

1.1.2.2. Simplifier version of specific form for capable users

More capable or trained users can insert an incident into a form of specific type, it's possible to define visible fields for them (e.g. loss for company can be evaluated later during solving of incident and is intended for managers of incident)

1.1.2.3. Automated import of data during insert or update of an incident

System can fetch data from external systems and prefill some inputs of a form. Data can be fetched according to values in fields. E.g. data about customer can be prefilled from your customer database according to their id or other identifying value.

1.1.2.4. Submitters can see their incidents and add comments

Submitters of incidents (who are not managers of incidents) can browse and search in "their" incidents and see details of incidents. They cannot update fields of incidents, but can append textual comments (e.g. on request of solving person who can see added comments).

1.1.3. User data loaded from Active Directory

List of users and their data (name, manager, function, contact, login name) can be loaded from Active Directory.

Users are automatically logged through NTLM protocol and domain control without filling login name and password.

1.1.4. Variety of access rights

There are several roles to define access rights

- for each incident types - insert, browse, update, see readonly details and reports, settings, open closed incidents
- administrator access – browse all incidents, manage general settings, view reports aggregated of all incidents

1.1.5. More languages

Now system has user interface in two languages, Czech and English, it's possible to add other ones.

System is ready to store and manage values in any language (Unicode support).

1.1.6. Notification emails

There are many predefined situation when notification emails are sent (e.g. inserting a new incident, change of solving person, guarded fields have extreme values), you can alter them to find your mid point between bothering and early warning. You can create new ones by setting conditions, text and recipients.

1.1.7. Solving persons, editing persons

There are two types of users who can update an incident

- Solving person is a "chief" for the incident and has responsibility for perfect solving of the incident, can close the incident
- Editing persons can update assigned incident

User can fill himself to be new solving persons, original solving person and managers of new and old solving person are notified.

Each type of incident has an implicit solving person being notified when a new incident is created.

1.1.8. Searching in incidents

It's possible to filter incidents according to various conditions

- Values including intervals (for date) in any field allowed to search in
- Fulltext search
- Fulltext search in attachments - files attached to incidents (in MS Word, MS Excel, PDF, text, html)

1.1.9. Similar values in incidents

There is a mechanism to find out similar values in incidents to find e.g. potentially same principals of malefaction. When user see detail or update an incident and system find other incidents with similar values, user is notified and can immediately look at similar incidents.

Similarity is evaluated according to user name, address, phone number, customer number, IMSI ...), conditions can be altered.

1.1.10. Reports

There are several predefined reports to analyze history of solving of incidents including graphs and export to MS Excel

- Numbers of incidents in defined periods, distinguishing types or department



- Submitting or solving persons
- Emergency incidents
- Car fleet incidents

1.1.11. Import, export incidents

Incidents can be imported from other systems, either through .NET Web service or special imports from files, emails, database including evaluating values and decision if it's incident or not and its level.

Incidents can be exported to other systems in various forms (records, reports, html or text details).

1.2. Technology

System is built on ASP.NET, MS SQL platform.

Necessary components on server are

- MS Windows 2003 Server, recent service pack (IIS, ASP.NET 2.0)
- MS SQL 2000, recent service pack
 - MS SQL Reporting Services, recent service pack
 - MS SQL Analysis services, recent service pack

MS SQL Reporting Services and MS SQL Analysis services are parts of MS SQL 2000.

Potentially it's possible to use MS SQL 2005.