



<b>Subject:</b>	Security Incidents startup specification
<b>Version:</b>	1.0
<b>Date:</b>	9.1.2008
<b>Author:</b>	Jan Klusáček, Jiří Helešic, Cyber Fox, s.r.o

## 1. Startup specification

Document describes startup conditions and comments to install and use Security Incident (SI) system.

We can split it to user interface (client part) and server part with application. Details of SI functionality are described in other documents.

### 1.1. User interface

Users can use the system through web browser, system is primarily designed for Internet Explorer 6 or higher but it is possible to prepare it for Mozilla browser (Mozilla, FireFox ...). It's not necessary to install anything on client site.

User is automatically logged and identified by NTLM authorization and Active Directory controller, data about users (name, email ...) are imported from Active Directory and can be joined with data from another source (e.g. HR database)

Common users should only know entry page to the system where they can insert general incident or navigate to other functionalities such as browsing in their submitted incidents or inserting some specific incident if they have access for it.

Administrators can go through the same entry page or they have other entry links to see and manage all or incidents of specific types.

### 1.2. Server

Now the system is ready to run on dedicated nonclustered server (including virtual machine) with these installed components

- 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.

The server is attached to domain and only authorized domain users can use the system. Server can connect to smtp or exchange server to send emails.

The system is regularly updating data about users from Active Directory and automatically inserts new user on the first login although the record has not been imported yet in regular import.

We expect that these operation on the server are provided by customer

- Administration and monitoring of the server - updates, service packs, monitoring of load
- Backups of the Windows and SI system – we can help to design backup and recovery plans

Cyber Fox developers monitor logs of SI to found or anticipate potential problems.

User rights are stored in database, based on groups of users.