Machine Readable Security Incident Notification

Vision (Small Project), Version 1.0

[Note: The following template is provided for use with the Rational Unified Process. Text enclosed in square brackets and displayed in blue italics (style=InfoBlue) is included to provide guidance to the author and should be deleted before publishing the document. A paragraph entered following this style will automatically be set to normal (style=Body Text).]

[To customize automatic fields in Microsoft Word (which display a gray background when selected), select File>Properties and replace the Title, Subject and Company fields with the appropriate information for this document. After closing the dialog, automatic fields may be updated throughout the document by selecting Edit>Select All (or Ctrl-A) and pressing F9, or simply click on the field and press F9. This must be done separately for Headers and Footers. Alt-F9 will toggle between displaying the field names and the field contents. See Word help for more information on working with fields.]

Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Version | Description | Author |
| 06/11/2014 | 1.0 | Creation | Hossein Fani |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

1. Introduction 4

1.1 References 4

2. Positioning 4

2.1 Problem Statement 4

2.2 Product Position Statement 4

3. Stakeholder and User Descriptions 5

3.1 Stakeholder Summary 5

3.2 User Summary 6

3.3 User Environment 6

3.4 Summary of Key Stakeholder or User Needs 6

3.5 Alternatives and Competition 6

4. Product Overview 6

4.1 Product Perspective 7

4.2 Assumptions and Dependencies 7

5. Product Features 7

6. Other Product Requirements 8

Vision (Small Project)

# Introduction

[The introduction of the **Vision** document provides an overview of the entire document. It includes the purpose and references of this **Vision** document.]

The purpose of this document is to collect, analyze, and define high-level needs and features of the “Machine Readable Security Incident Notification”. It focuses on the capabilities needed by the stakeholders and the target users, and why these needs exist. The details of how the “Machine Readable Security Incident Notification” fulfills these needs are detailed in the use-case and supplementary specifications.

## References

[This subsection provides a complete list of all documents referenced elsewhere in the **Vision** document. Identify each document by title, report number if applicable, date, and publishing organization. Specify the sources from which the references can be obtained. This information may be provided by reference to an appendix or to another document.]

# Positioning

## Problem Statement

[Provide a statement summarizing the problem being solved by this project. The following format may be used:]

|  |  |
| --- | --- |
| The problem of | [describe the problem]  Ryerson University security incident notification are not machine readable |
| affects | [the stakeholders affected by the problem]  Hossein Fani, Student |
| the impact of which is | [what is the impact of the problem?]  Automatic knowledge extraction and mining of incidents is impossible. |
| a successful solution would be | [list some key benefits of a successful solution]   * Security incidents is represented in Semantic Web way * An ontology for security incidents is proposed * Extraction and Semantic Web representation is automatic * Dashboard of statistical diagrams and real-time monitoring is provided |

## Product Position Statement

[Provide an overall statement summarizing, at the highest level, the unique position the product intends to fill in the marketplace. The following format may be used:]

|  |  |
| --- | --- |
| For | [target customer]   1. Ryerson University 2. Toronto Police Service |
| Who | [statement of the need or opportunity]   1. Believes an informed community is a safer one. 2. Monitors and analyze the security incidents and provide precautionary programs |
| The “Machine Readable Security Incident” | is a [product category]  Semantic Web Enabled Data Mart |
| That | [statement of key benefit; that is, the compelling reason to buy]  Machine readable security incident representation |
| Unlike | [primary competitive alternative]  No competitive alternative |
| Our product | [statement of primary differentiation]  Automatically extract security incident information and provide machine readable representation |

[A product position statement communicates the intent of the application and the importance of the project to all concerned personnel.]

# Stakeholder and User Descriptions

[To effectively provide products and services that meet your stakeholders’ and users' real needs it is necessary to identify and involve all of the stakeholders as part of the Requirements Modeling process. You must also identify the users of the system and ensure that the stakeholder community adequately represents them. This section provides a profile of the stakeholders and users involved in the project, and the key problems that they perceive to be addressed by the proposed solution. It does not describe their specific requests or requirements as these are captured in a separate stakeholder requests artifact. Instead, it provides the background and justification for why the requirements are needed.]

## Stakeholder Summary

[There are a number of stakeholders with an interest in the development and not all of them are end users. Present a summary list of these non-user stakeholders. (The users are summarized in section 3.2.)]

|  |  |  |
| --- | --- | --- |
| **Name** | **Description** | **Responsibilities** |
| [Name the stakeholder type.]  Developer | [Briefly describe the stakeholder.]  Hossein Fani | [Summarize the stakeholder’s key responsibilities with regard to the system being developed; that is, their interest as a stakeholder. For example, this stakeholder: ensures that the system will be maintainable, ensures that there will be a market demand for the product’s features, monitors the project’s progress, approves funding, and so forth]  Implement the product. |

## User Summary

[Present a summary list of all identified users.]

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Description** | **Responsibilities** | **Stakeholder** |
| [Name the user type.] | [Briefly describe what they represent with respect to the system.]  Dr. Ebrahim Bagheri | [List the user’s key responsibilities with regard to the system being developed; for example: captures details, produces reports, coordinates work, and so on] | [If the user is not directly represented, identify which stakeholder is responsible for representing the user’s interest.] |

## User Environment

[Detail the working environment of the target user. Here are some suggestions:

Number of people involved in completing the task? Is this changing?

How long is a task cycle? Amount of time spent in each activity? Is this changing?

Any unique environmental constraints: mobile, outdoors, in-flight, and so on?

Which system platforms are in use today? Future platforms?

What other applications are in use? Does your application need to integrate with them?

This is where extracts from the Business Model could be included to outline the task and roles involved, and so on.]

## Summary of Key Stakeholder or User Needs

[List the key problems with existing solutions as perceived by the stakeholder or user. Clarify the following issues for each problem:

• What are the reasons for this problem?

• How is it solved now?

• What solutions does the stakeholder or user want?]

[It is important to understand the **relative** importance the stakeholder or user places on solving each problem. Ranking and cumulative voting techniques indicate problems that **must** be solved versus issues they would like addressed.

Fill in the following table—if using Rational RequisitePro to capture the Needs, this could be an extract or report from that tool.]

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Need** | **Priority** | **Concerns** | **Current Solution** | **Proposed Solutions** | |
|  |  |  |  | |  |

## Alternatives and Competition

[Identify alternatives the stakeholder perceives as available. These can include buying a competitor’s product, building a homegrown solution, or simply maintaining the status quo. List any known competitive choices that exist or may become available. Include the major strengths and weaknesses of each competitor as perceived by the stakeholder or end user.]

# Product Overview

[This section provides a high level view of the product capabilities, interfaces to other applications, and system configurations. This section usually consists of two subsections, as follows:

• Product perspective

• Assumptions and dependencies]

## Product Perspective

[This subsection of the **Vision** document puts the product in perspective to other related products and the user’s environment. If the product is independent and totally self-contained, state it here. If the product is a component of a larger system, then this subsection needs to relate how these systems interact and needs to identify the relevant interfaces between the systems. One easy way to display the major components of the larger system, interconnections, and external interfaces is with a block diagram.]

Ryerson University believes an informed community is a safer one. The Integrated Risk Management (IRM) system notifies all Ryerson staff, students, faculty and alumni (who have graduated within the past five years) by security incident alarms which are delivered directly via email. For the urban campus is located at the downtown center of Toronto, the most populous, yet commercial capital city in Canada, such system seems indispensable to continually enhance the safety and security of the community. Each notification includes temporal facts of the incident, location, victim and suspect details, and a brief account of whole event. However, incident records are expressed in diverse and application dependent formats which impedes common comprehension for automatic knowledge extraction and reasoning. In this project, we develop a Semantic Web use case to help security incident notifications machine readable. To do so, we devise a novel light-weight domain ontology for security incidents, namely SIO. Next, we automatically extract information from textual content of security incident notification by annotating the temporal and eventual facts of incidents (extraction), and store the information based on SIO in a triple store (transform). Finally, we develop a data mart to provide knowledge through dashboard of statistical diagrams and gages (load). These extraction, transform, and load phases constitute a real-time ETL engine which receives textual incident notifications as input and summarize them into visual diagrams.

This project not only provides profound knowledge of steps in applying Semantic Web representation of information in Word Wide Web to the developers, but also produces SIO, an ontology for describing security incidents from indecent behavior to assault to more adverse crime which raise the security alarm in a community. SIO will present a unique way to the security incident detectors, a police officer, Robocops, or intelligent CCTV cameras, to report machine readable security events. Furthermore, to our knowledge, there is no real-time security incident data mart based on triple structure representation thus far. Related works are mainly follow OLAP approaches which rely on relational representation of information and are dramatically different from Semantic Web way of providing information.

This project is developed as a final project for EE8605: Semantic Web Technologies as a graduate course in fall 2014, Department of Electrical and Computer Engineering Department, Ryerson University, Toronto, Ontario, Canada. OWL 2 and WebProtégé is the ontology language and editor respectively, Virtuoso is our triple store, and SPARQL is the query and data manipulation language.

|  |
| --- |
|  |

|  |  |
| --- | --- |
|  |  |
|  |
| http://www.sinnexus.com/images/datamart_example.jpg |

## Assumptions and Dependencies

[List each factor that affects the features stated in the **Vision** document. List assumptions that, if changed, will alter the **Vision** document. For example, an assumption may state that a specific operating system will be available for the hardware designated for the software product. If the operating system is not available, the **Vision** document will need to change.]

Our work highly relies on the security incidents notification as source. That means that the notification should be accessible and includes temporal and eventual facts in the body. The notification language is assumed English.

# Product Features

[List and briefly describe the product features. Features are the high-level capabilities of the system that are necessary to deliver benefits to the users. Each feature is an externally desired service that typically requires a series of inputs to achieve the desired result. For example, a feature of a problem tracking system might be the ability to provide trending reports. As the use-case model takes shape, update the description to refer to the use cases.

Because the **Vision** document is reviewed by a wide variety of involved personnel, the level of detail needs to be general enough for everyone to understand. However, enough detail must be available to provide the team with the information they need to create a use-case model.

To effectively manage application complexity, we recommend for any new system, or an increment to an existing system, capabilities be abstracted to a high enough level so 25-99 features result. These features provide the fundamental basis for product definition, scope management, and project management. Each feature will be expanded in greater detail in the use-case model.

Throughout this section, each feature will be externally perceivable by users, operators, or other external systems. These features should include a description of functionality and any relevant usability issues that must be addressed. The following guidelines apply:

• Avoid design. Keep feature descriptions at a general level. Focus on capabilities needed and why (not how) they should be implemented.

• If you are using the Rational RequisitePro toolkit, all need to be selected as requirements of type for easy reference and tracking.]

[Define the priority of the different system features. Include, if useful, attributes such as stability, benefit, effort, and risk.]

The security incident information is extracted automatically by processing the textual content of the notification. This extraction step is preliminary to the next steps.

An ontology for security incidents is devised, namely SIO. This step is done parallel to the extraction step since the content of the notification provide the data as well as meta-data.

With SIO in hand, we store the extracted information in triple structure in a triple store engine, specifically Virtuoso.

The last phase is implementing a web-base data mart to draw general statistics about the incidents and online monitoring as well.

# Other Product Requirements

[At a high level, list applicable standards, hardware, or platform requirements; performance requirements; and environmental requirements.

Define the quality ranges for performance, robustness, fault tolerance, usability, and similar characteristics that are not captured in the Feature Set.

Note any design constraints, external constraints, or other dependencies.

Define any specific documentation requirements, including user manuals, online help, installation, labeling, and packaging requirements.

Define the priority of these other product requirements. Include, if useful, attributes such as stability, benefit, effort, and risk.]