UNIVERSITY OF SANTIAGO DE COMPOSTELA

ESCOLA TÉCNICA SUPERIOR DE ENXEÑARÍA

Improvements in IDS: adding functionality to Wazuh

Autor:
Andrés Santiago Gómez Vidal

Directores:
Purificación Cariñena Amigo
Andrés Tarascó Acuña

Computer Engineering Degree

February 2019

Final degree project presented at the Escola Técnica Superior de Enxeñaría of the University of Santiago de Compostela to obtain the Degree in Computer Engineering

Ms. Purificación Cariñena Amigo, Professor Computing Science and Artificial Intelligence at the University of Santiago de Compostela and **Mr. Andrés Tarascó Acuña**, Managing Director at Tarlogic Security S.L.

STATE:

That the present report entitled *Improvements in IDS: adding functionality to Wazuh* written by **Andrés Santiago Gómez Vidal** in order to obtain the ECTS corresponding to the final degree project of the Computer Engineering degree was conducted under our direction in the department of Computer Science and Artificial Intelligence of the University of Santiago de Compostela.

For the purpose to be duly recorded, this document was signed in Santiago de Compostela on February TODO, 2019:

The director, The codirector, The student,

(Purificación Cariñena Amigo) (Andrés Tarascó Acuña) (Andrés Gómez Vidal)

Index

List of Figures

List of Tables

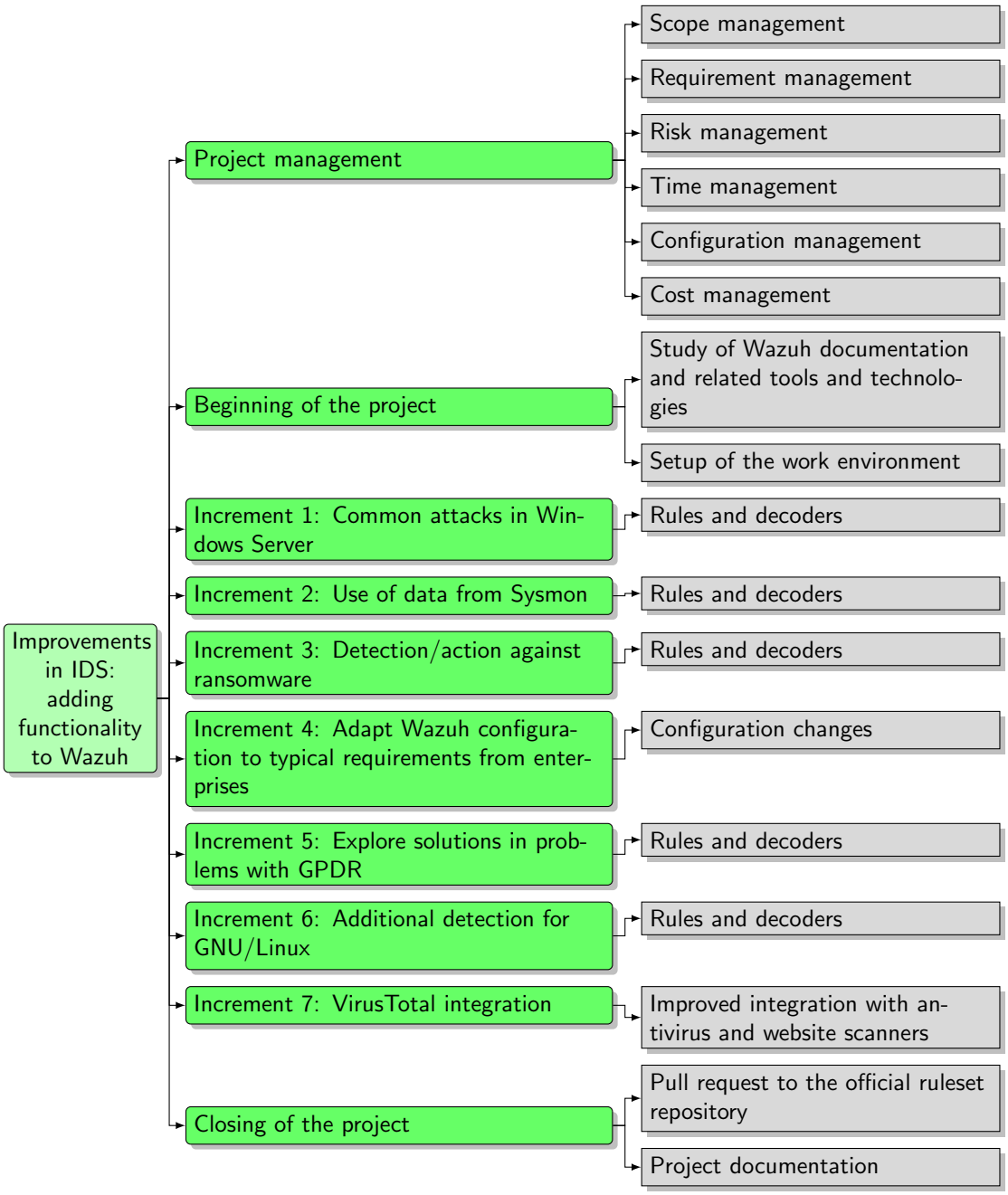
Chapter 1

Introdución

Chapter 2

Panning

2.1 Initial WBS



2.2 Initial planning

2.3 Final planning

Chapter 3

Requirements

Chapter 4

Design

Chapter 5

Conclusions and additions

5.1 Risk management

5.1.1 Risk metrics

5.1.2 Risk types

5.1.3 Risk identification

Table 5.1: Project risks

Identifier	Name
R-000	Optimist planning, "best case" (instead of a realistic "expected case")
R-000	Bad requirement specification
R-000	Design errors
R-000	Lack of key information from sources
R-000	Lack of feedback or support from the security consultants of Tarlogic
R-000	The learning curve of some technologies is larger than expected
R-000	The unexplained parts of the project take more time than expected
R-000	Cannot access source material
R-000	Unexpected changes in any of the APIs used in the project
R-000	Loss of work
R-000	Wrong management of the project's configuration
R-000	A delay in one task leads to cascading delays in the dependent tasks
R-000	Unnecesary work
R-000	The quality of the product is not enough
R-000	Sickness or overwork
R-000	Performance issues

5.1.4 Risk analysis

Identifier	**R-000**
Description	Bla bla bla bla bla bla bla bla bla bla bla bla bla Bla bla bla bla bla bla bla bla bla bla bla bla bla bla bla Bla bla bla bla bla bla bla bla bla bla bla bla bla
Probability	Low , Medium , High
Impact	Low , Medium , High
Exposition	Low , Medium , High
Indicator	Bla bla bla bla bla bla bla bla bla bla bla bla bla

Identifier	**R-001**
Description	
Probability	
Impact	
Exposition	
Indicator	

5.1.5 Risk planning

5.1.6 Risk supervision

Appendix A

Manuais técnicos

Manuais técnicos: en función do tipo de Traballo e metodoloxía empregada, o contido poderase dividir en varios documentos. En todo caso, neles incluirase toda a información precisa para aquelas persoas que se vaian a encargar do desenvolvemento e/ou modificación do Sistema (por exemplo código fonte, recursos necesarios, operacións necesarias para modificacións e probas, posibles problemas, etc.). O código fonte poderase entregar en soporte informático en formatos PDF ou postscript.

Appendix B

Manuais de usuario

Manuais de usuario: incluirán toda a información precisa para aquelas persoas que utilicen o Sistema: instalación, utilización, configuración, mensaxes de erro, etc. A documentación do usuario debe ser autocontida, é dicir, para o seu entendemento o usuario final non debe precisar da lectura de outro manual técnico.

Appendix C

Licenza

Se se quere pór unha licenza (GNU GPL, Creative Commons, etc), o texto da licenza vai aquí.