

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

1	Introducción	1
2	Planning	3
2.1	Initial WBS	3
2.2	Initial planning	4
2.3	Final planning	4
3	Requirements	5
4	Design	7
5	Conclusions and additions	9
5.1	Risk management	11
5.1.1	Risk metrics	11
5.1.2	Risk types	11
5.1.3	Risk identification	11
5.1.4	Risk analysis	11
5.1.5	Risk planning	12
5.1.6	Risk supervision	12
A	Manuais técnicos	13
B	Manuais de usuario	15
C	Licenza	17

List of Figures

List of Tables

5.1	Project risks	11
-----	-------------------------	----

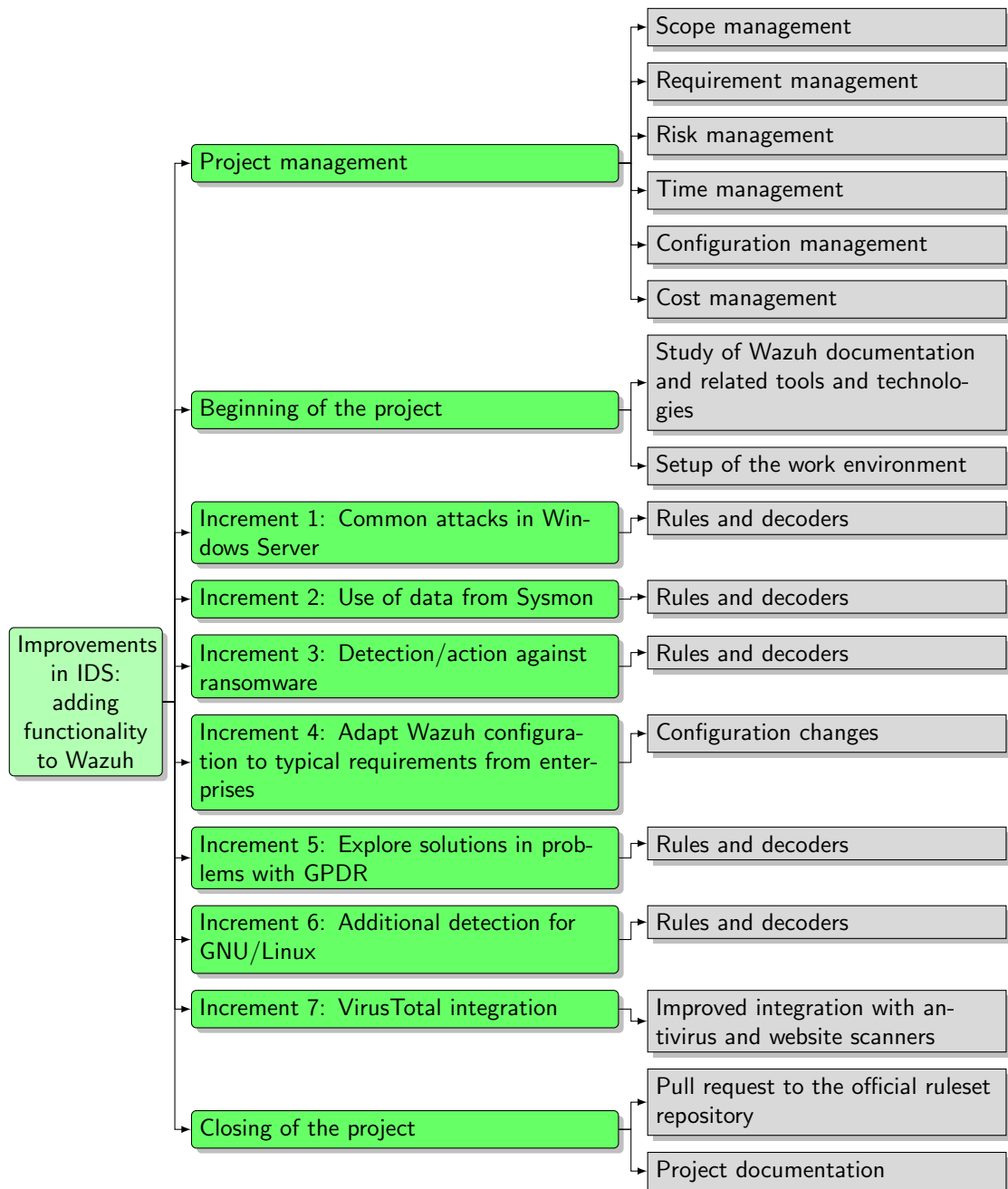
Chapter 1

Introducción

Chapter 2

Planning

2.1 Initial WBS



2.2 Initial planning

2.3 Final planning

Chapter 3

Requirements

Chapter 4

Design

Chapter 5

Conclusions and additions

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 incluírase 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: incluírán 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.

