



# *Threat Hunting* basado en técnicas de Inteligencia Artificial

Autor:  
Mario Aragonés Lozano

Director:  
Dr. Manuel Esteve Domingo  
Dr. Israel Pérez Llopis

## Índice

Resumen	I
Resum	III
Abstract	V
Índice general	VII
Índice de figuras	XI
Índice de tablas	XIII
Índice de códigos	XV
Siglas	XVII
<b>1 Introducción y objetivos</b>	<b>1</b>
1.1 Introducción . . . . .	1
1.2 Objetivos . . . . .	4
1.3 Principales aportaciones . . . . .	5
1.3.1 Artículos de revista . . . . .	5
1.3.2 Publicaciones en congresos . . . . .	5
1.3.3 Participación en proyectos de investigación . . . . .	6
1.4 Estructura de la memoria . . . . .	6
<b>2 Estado del arte</b>	<b>7</b>
2.1 Soluciones actuales . . . . .	7
2.2 Arquitecturas de aplicación . . . . .	10
2.2.1 Monolíticas . . . . .	12
2.2.2 Distribuidas . . . . .	13
2.3 Mecanismos de comunicación . . . . .	16
2.3.1 Paradigmas de comunicación . . . . .	16
2.3.2 Protocolos de intercambio de información . . . . .	18

2.4	Recursos actuales . . . . .	21
2.4.1	Adquisición de los datos . . . . .	22
2.4.2	Modelado de los datos . . . . .	23
2.4.3	Preparación de los datos para Inteligencia Artificial . . . . .	24
2.4.4	Procesado de los datos mediante Inteligencia Artificial . . . . .	27
2.4.5	Intercambio de los datos . . . . .	38
2.4.6	Interacción con los datos . . . . .	40
2.5	Servicios actuales . . . . .	47
2.5.1	Almacenamiento de los datos . . . . .	48
2.5.2	Interacción entre componentes . . . . .	52
2.5.3	Gestión de la autenticación y la autorización . . . . .	54
<b>3</b>	<b>Propuesta de arquitectura</b>	<b>59</b>
3.1	Conjunto de componentes de los datos . . . . .	61
3.1.1	Recolección . . . . .	62
3.1.2	Procesamiento y almacenamiento . . . . .	65
3.1.3	Preparación y configuración . . . . .	70
3.1.4	Presentación . . . . .	74
3.2	Conjunto de componentes de los recursos . . . . .	77
3.2.1	Comunicaciones . . . . .	77
3.2.2	Gestión de la autenticación y de la autorización . . . . .	78
<b>4</b>	<b>Validación y verificación de la arquitectura</b>	<b>79</b>
4.1	Prototipo . . . . .	80
4.1.1	Infraestructura . . . . .	80
4.1.2	Lenguaje de programación . . . . .	81
4.1.3	Conjunto de componentes de los datos . . . . .	81
4.1.4	Conjunto de componentes de los recursos . . . . .	89
4.2	Validación . . . . .	90
4.2.1	Conjunto de componentes de los datos . . . . .	91
4.3	Verificación en entorno controlado . . . . .	95
4.3.1	Primer caso de uso . . . . .	96
4.3.2	Segundo caso de uso . . . . .	98
4.3.3	Tercer caso de uso . . . . .	100
4.3.4	Cuarto caso de uso . . . . .	102
4.3.5	Quinto caso de uso . . . . .	105
4.3.6	Sexto caso de uso . . . . .	107
4.4	Verificación en entorno no controlado: PRAETORIAN . . . . .	110
<b>5</b>	<b>Conclusiones y trabajos futuros</b>	<b>119</b>
5.1	Conclusiones . . . . .	119
5.2	Trabajos futuros . . . . .	121
	<b>Bibliografía</b>	<b>125</b>