Lumberjack Partial Presentation

19/04/2024 Group 8

wazuh.

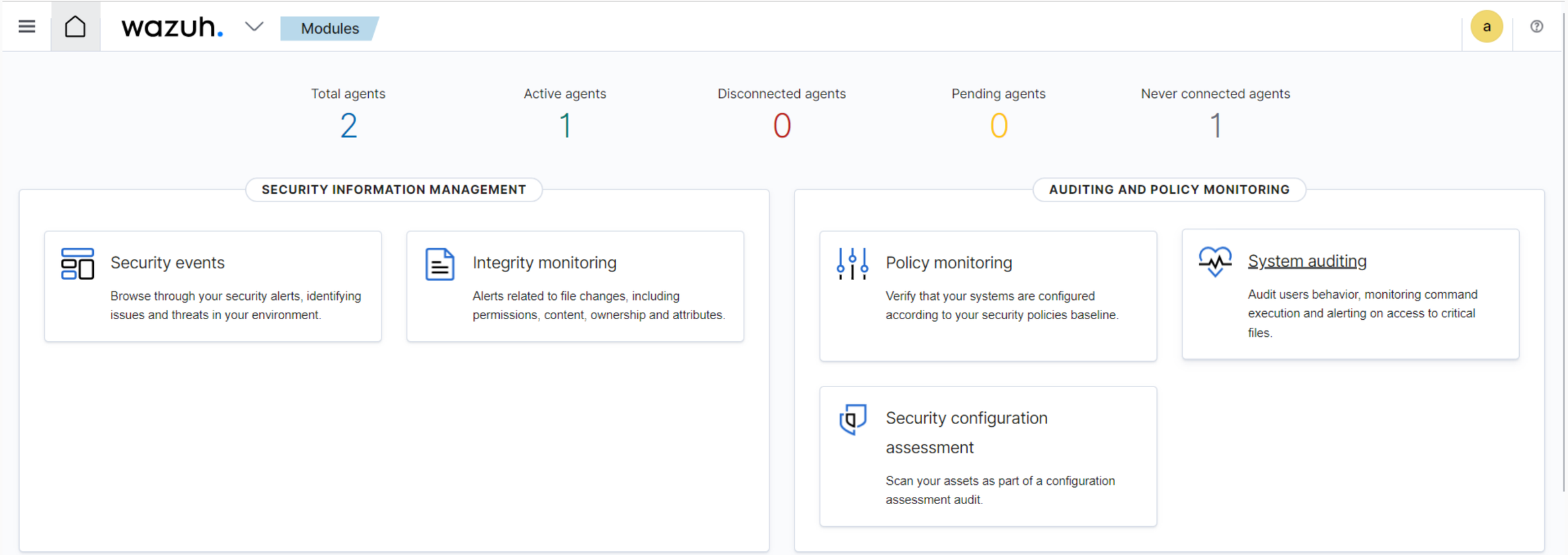
First Attempt Everything Together

- Not familiarized
- Bad Idea

Simulate a Server as our agent.

- IPs troubles when installing an agent, we had difficulties to connect again. Maybe because of the vm environment.
- Injection of logs still a challenge

Ubuntu Server


wazuh.
Modules
a
Total agents
2
Active agents
1
Disconnected agents
0
Pending agents
0
Never connected agents
1
SECURITY INFORMATION MANAGEMENT
Security events
Browse through your security alerts, identifying issues and threats in your environment.
Integrity monitoring
Alerts related to file changes, including permissions, content, ownership and attributes.
AUDITING AND POLICY MONITORING
Policy monitoring
Verify that your systems are configured according to your security policies baseline.
System auditing
Audit users behavior, monitoring command execution and alerting on access to critical files.
Security configuration assessment
Scan your assets as part of a configuration assessment audit.

STATUS

- Active (1)
- Disconnected (0)
- Pending (0)
- Never connected (1)

DETAILS

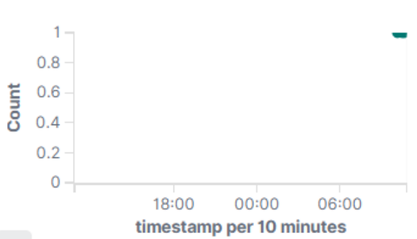
Active	Disconnected	Pending	Never connected	Agents coverage
1	0	0	1	50.00%

Last registered agent
server

Most active agent
server

EVOLUTION

Last 24 hours



Agents (2)

Deploy new agent | Refresh | Export formatted

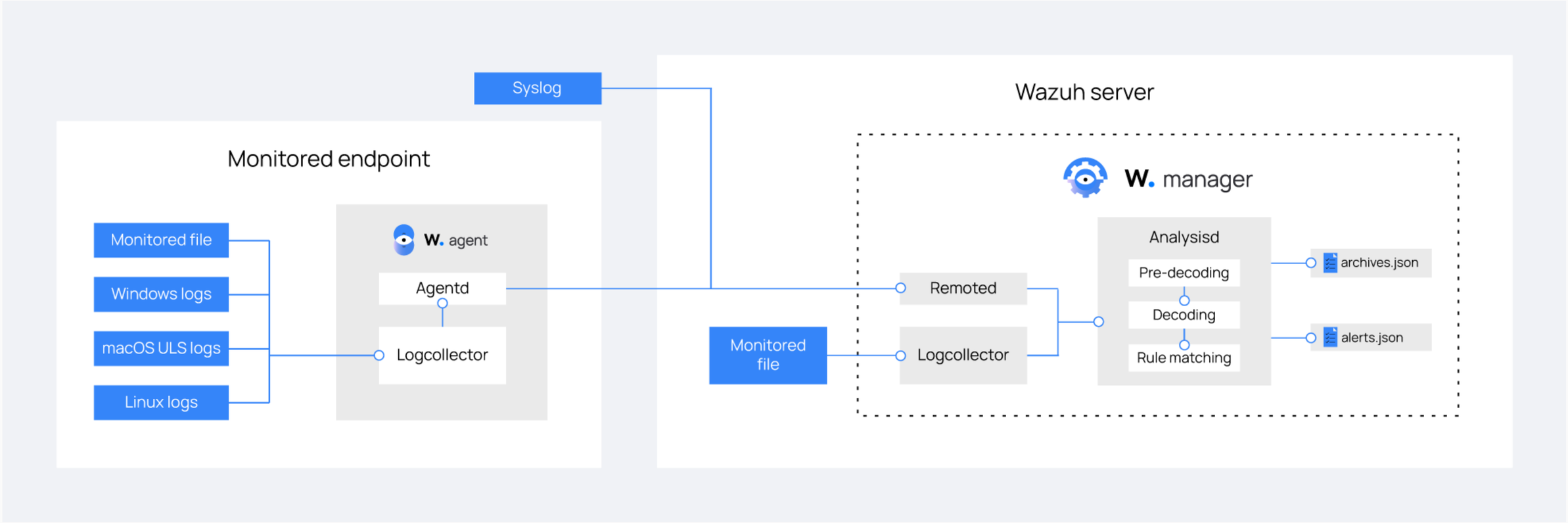
id!=000 and | Search | WQL | Refresh

ID	Name	IP address	Group(s)	Operating system	Cluster node	Version	Status	Actions
001	test	any		-	-	-	never connected	
002	server	192.168.86.138	default	Ubuntu 22.04.4 LTS	node01	v4.7.3	active	

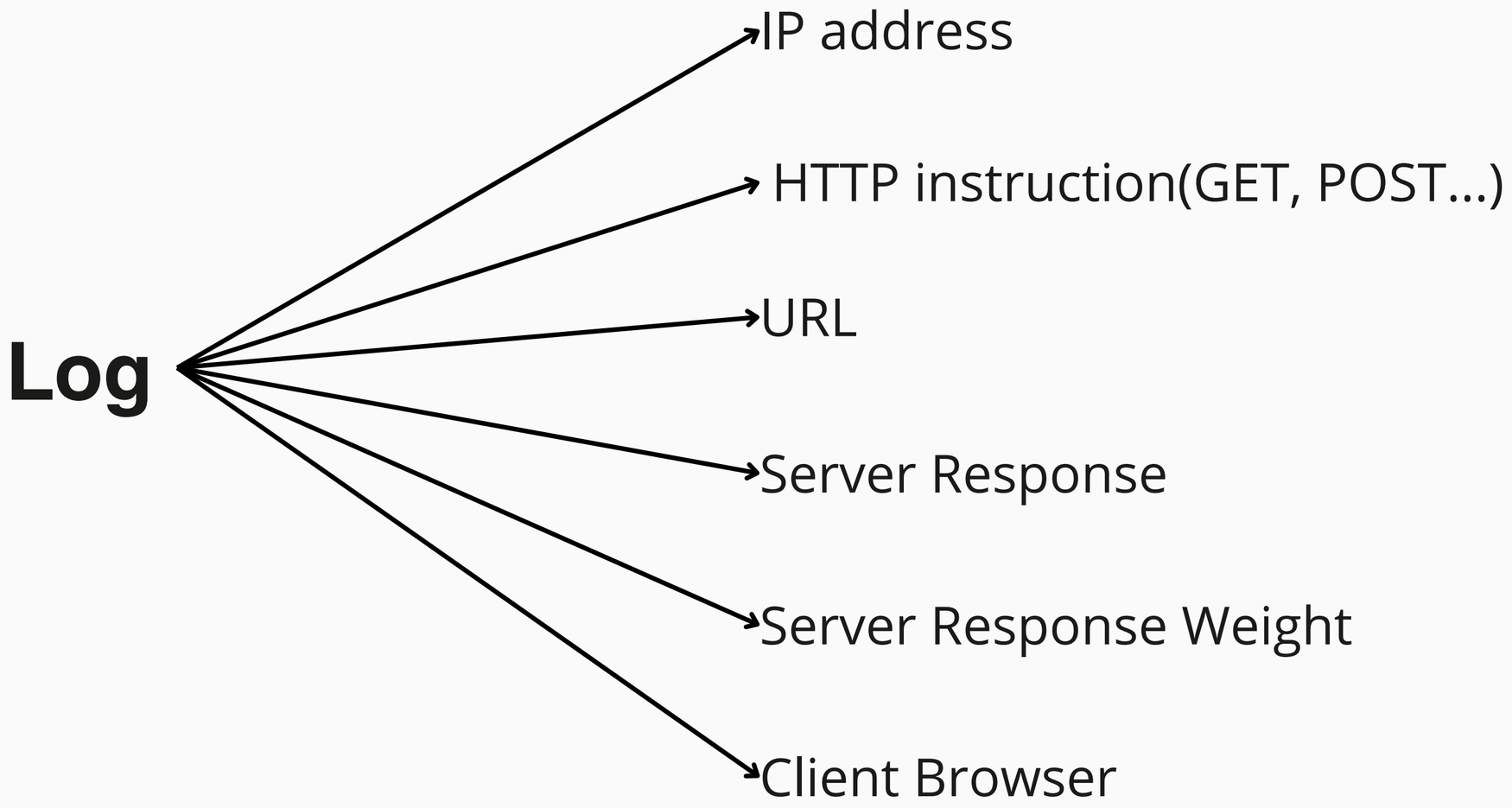
Rows per page: 10

1

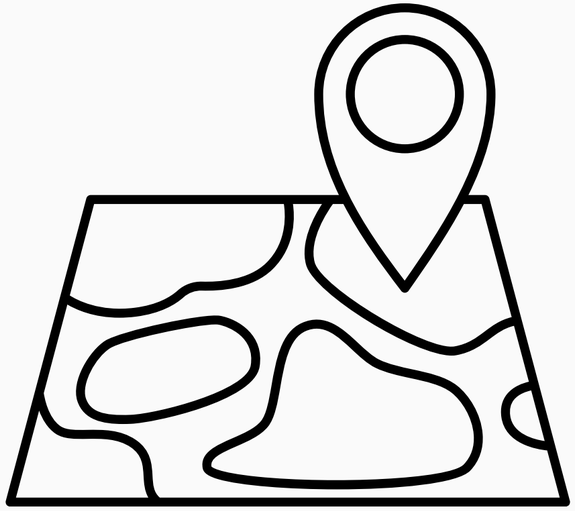
Future Challenges



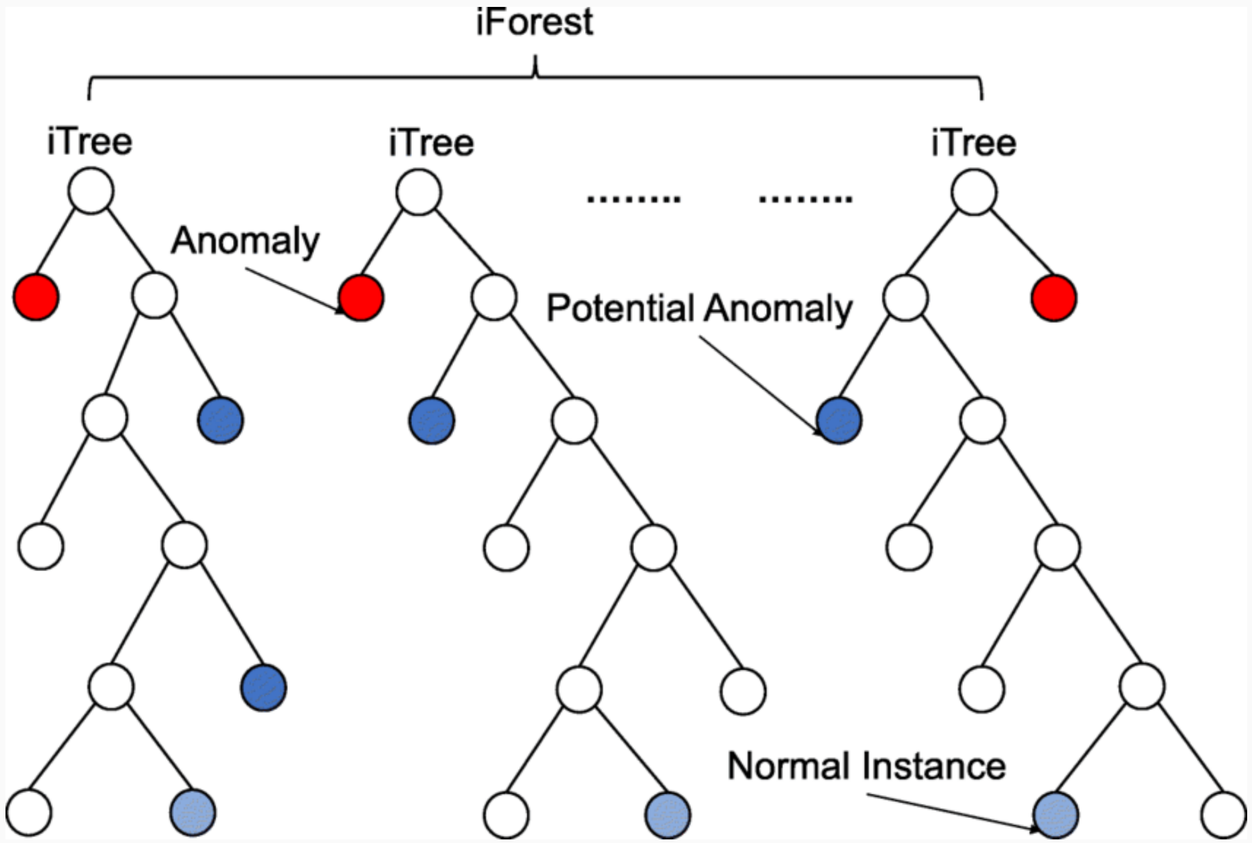
Segmentation



Feature Extraction

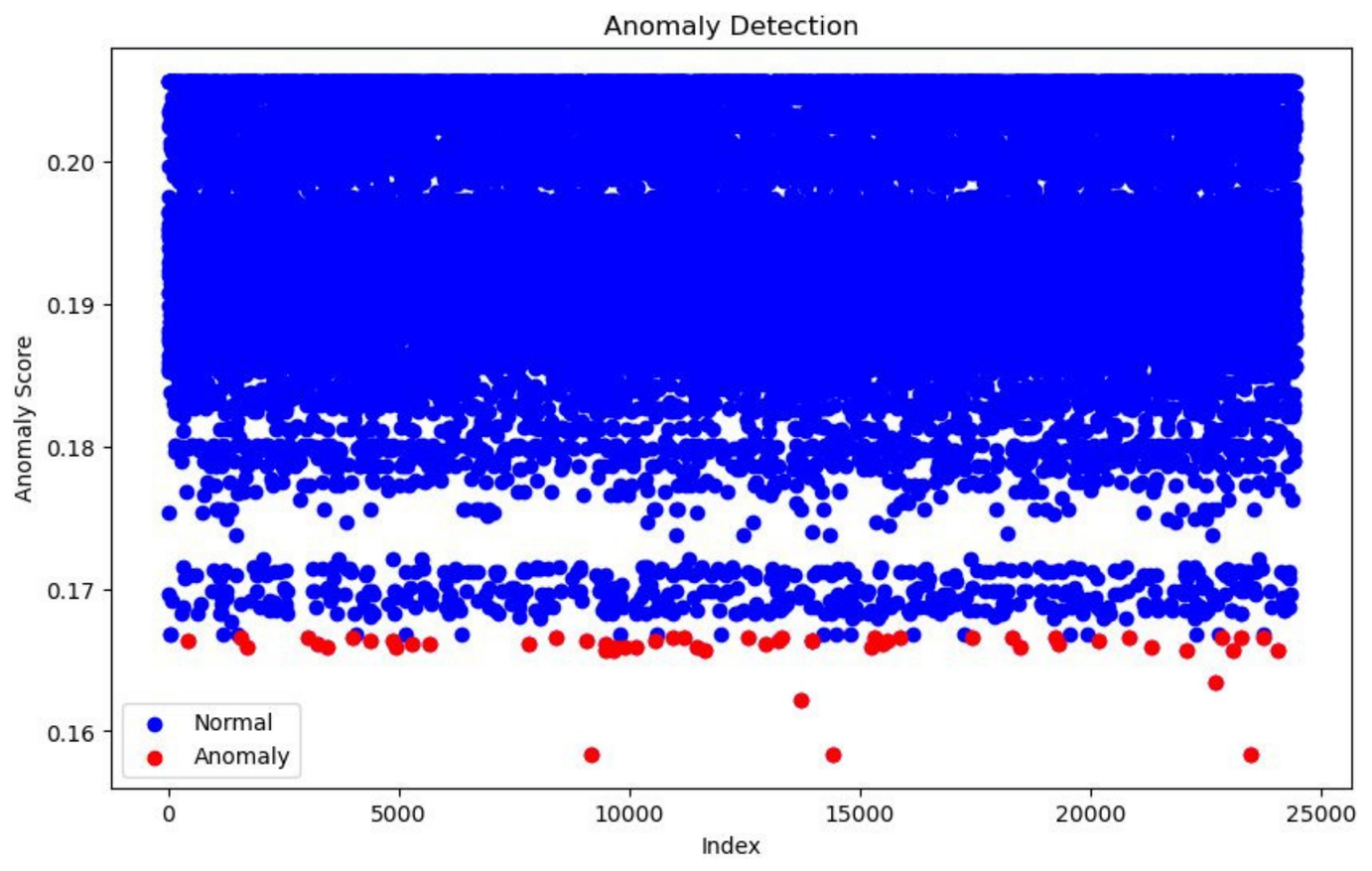


Our Current Approach: Isolation Forest



Unsupervised Learning

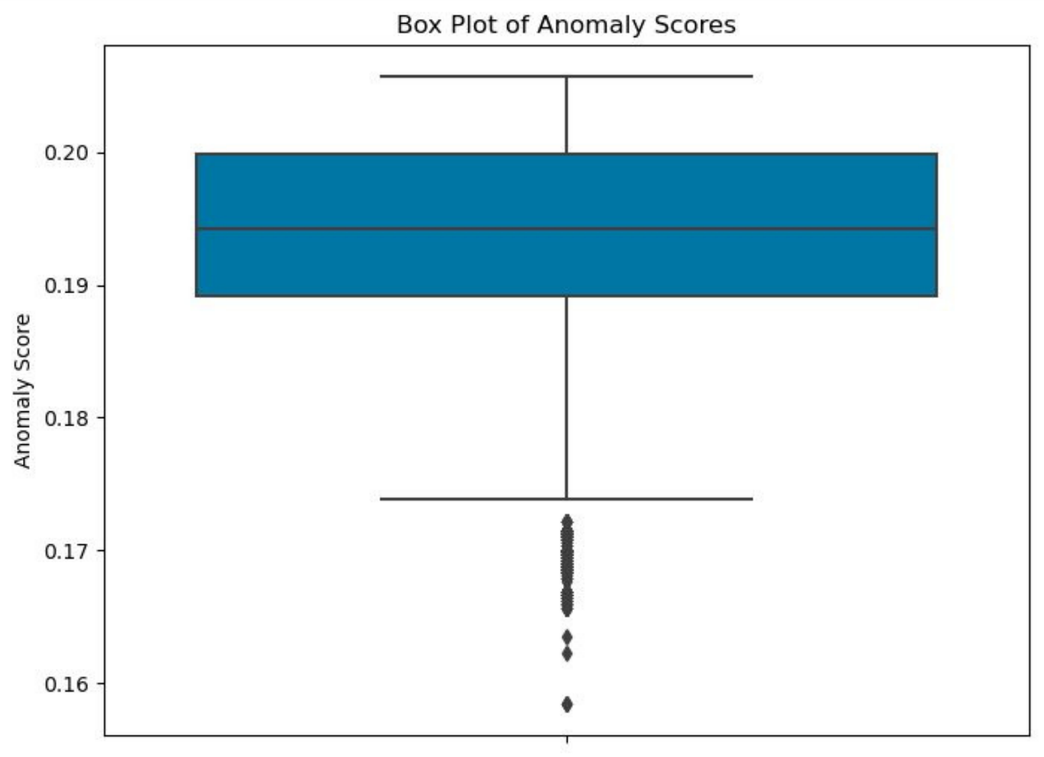
What we have until now



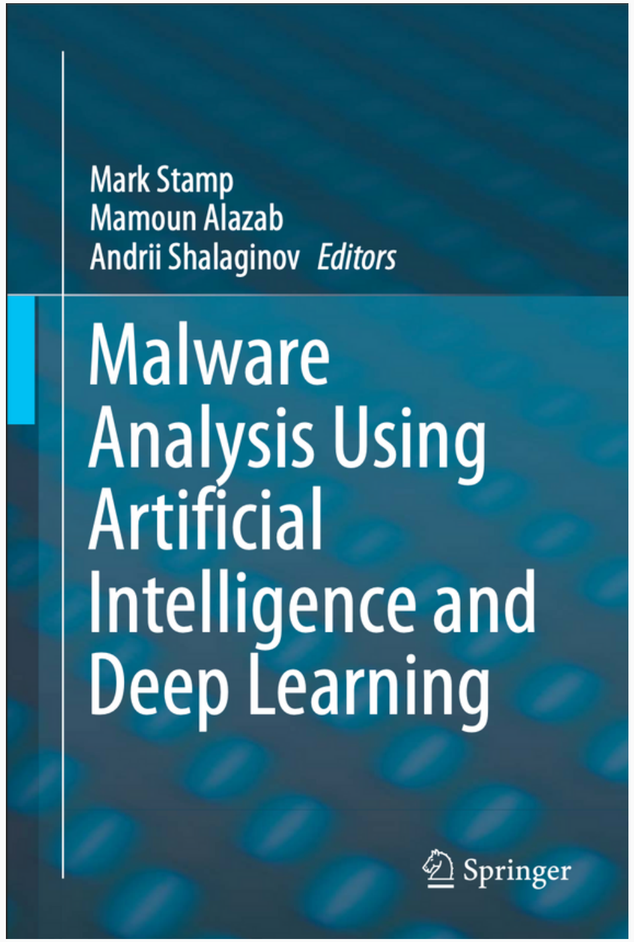
- 0,25 percentile threshold (not definitive)
- No fine-tuning
- **No evaluation**

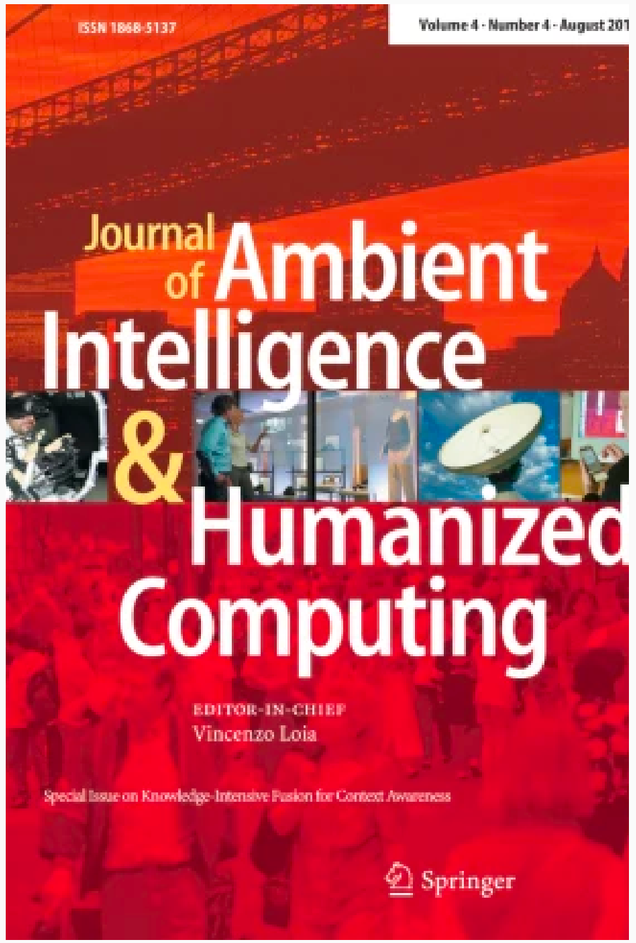
Main Difficulties

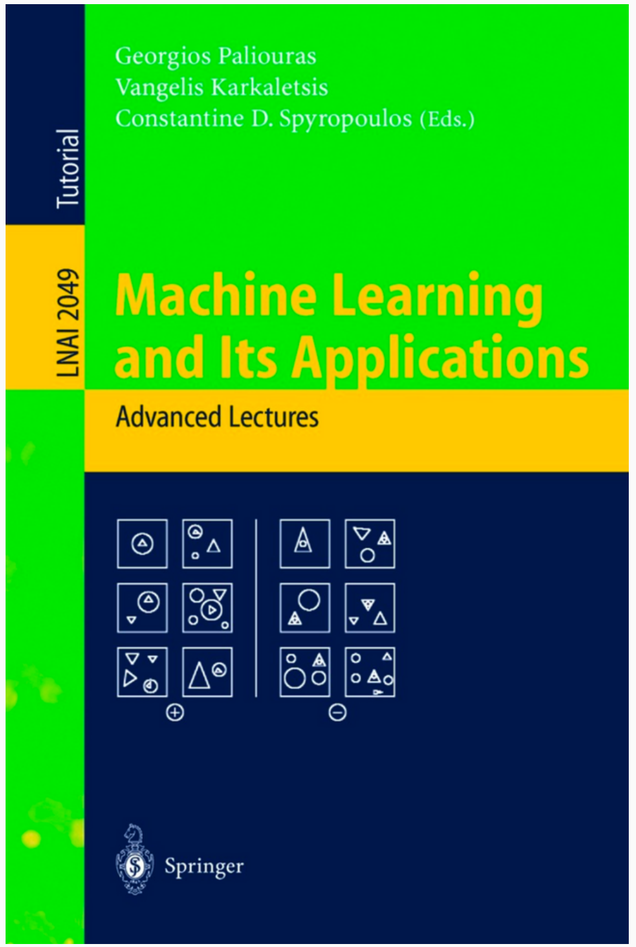
- No proper way of evaluating (lack of feedback)
- More features needed
- Some features were dropped (IP, coordinates...)



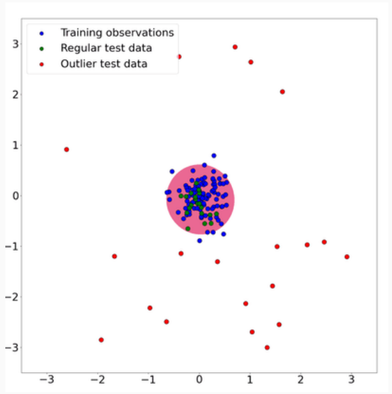
What’s next?

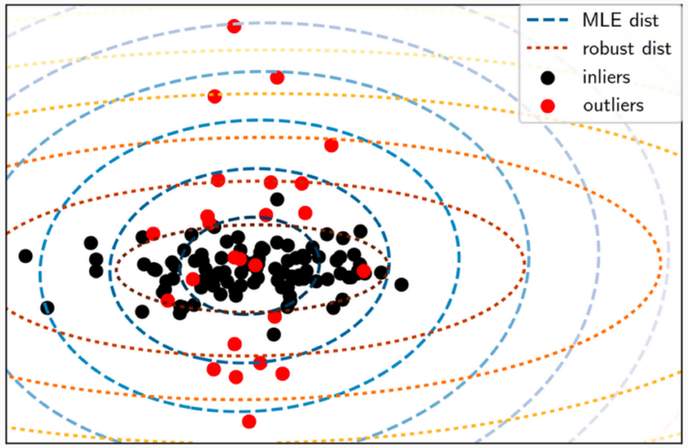

Mark Stamp
Mamoun Alazab
Andrii Shalaginov Editors
Malware Analysis Using Artificial Intelligence and Deep Learning
Springer

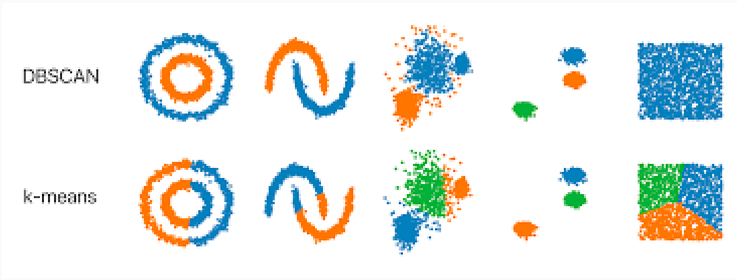

ISSN 1868-5137
Volume 4 · Number 4 · August 201
Journal of Ambient Intelligence & Humanized Computing
EDITOR-IN-CHIEF
Vincenzo Loia
Special Issue on Knowledge-Intensive Fusion for Context Awareness
Springer

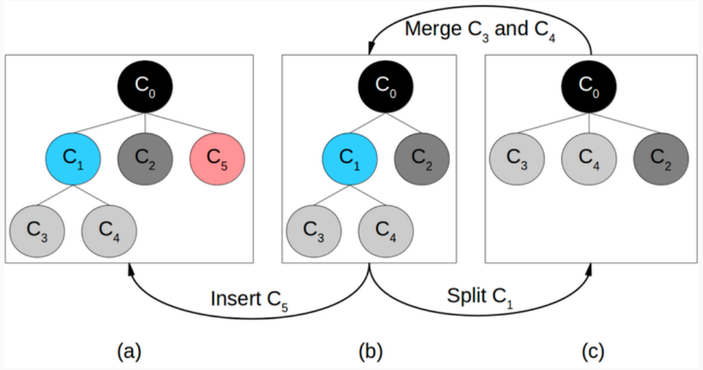

Tutorial
LNAI 2049
Georgios Paliouras
Vangelis Karkaletsis
Constantine D. Spyropoulos (Eds.)
Machine Learning and Its Applications
Advanced Lectures
Springer

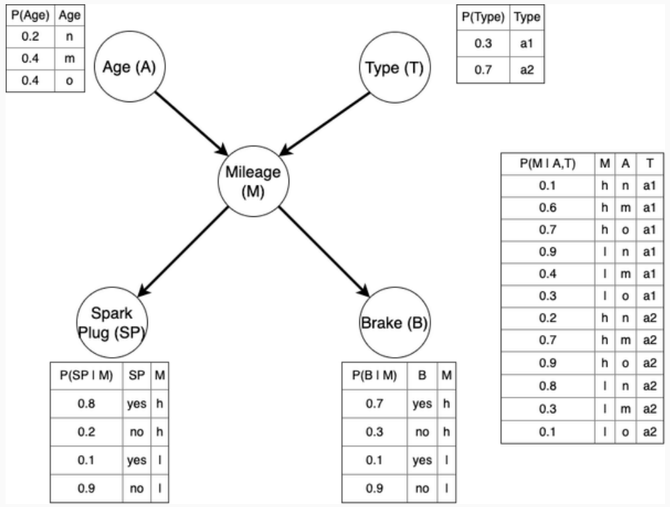
Model Mania











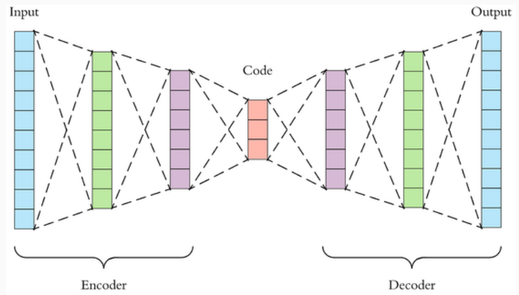
P(Age)	Age
0.2	n
0.4	m
0.4	o

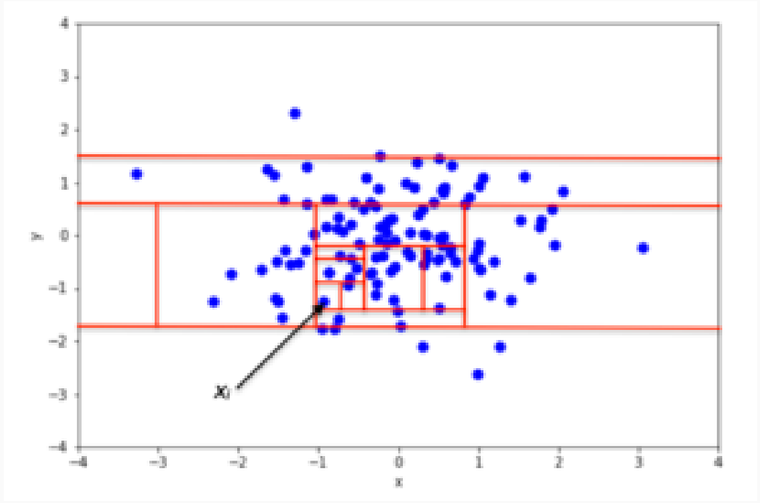
P(Type)	Type
0.3	a1
0.7	a2

P(SP | M)	SP	M
0.8	yes	h
0.2	no	h
0.1	yes	l
0.9	no	l

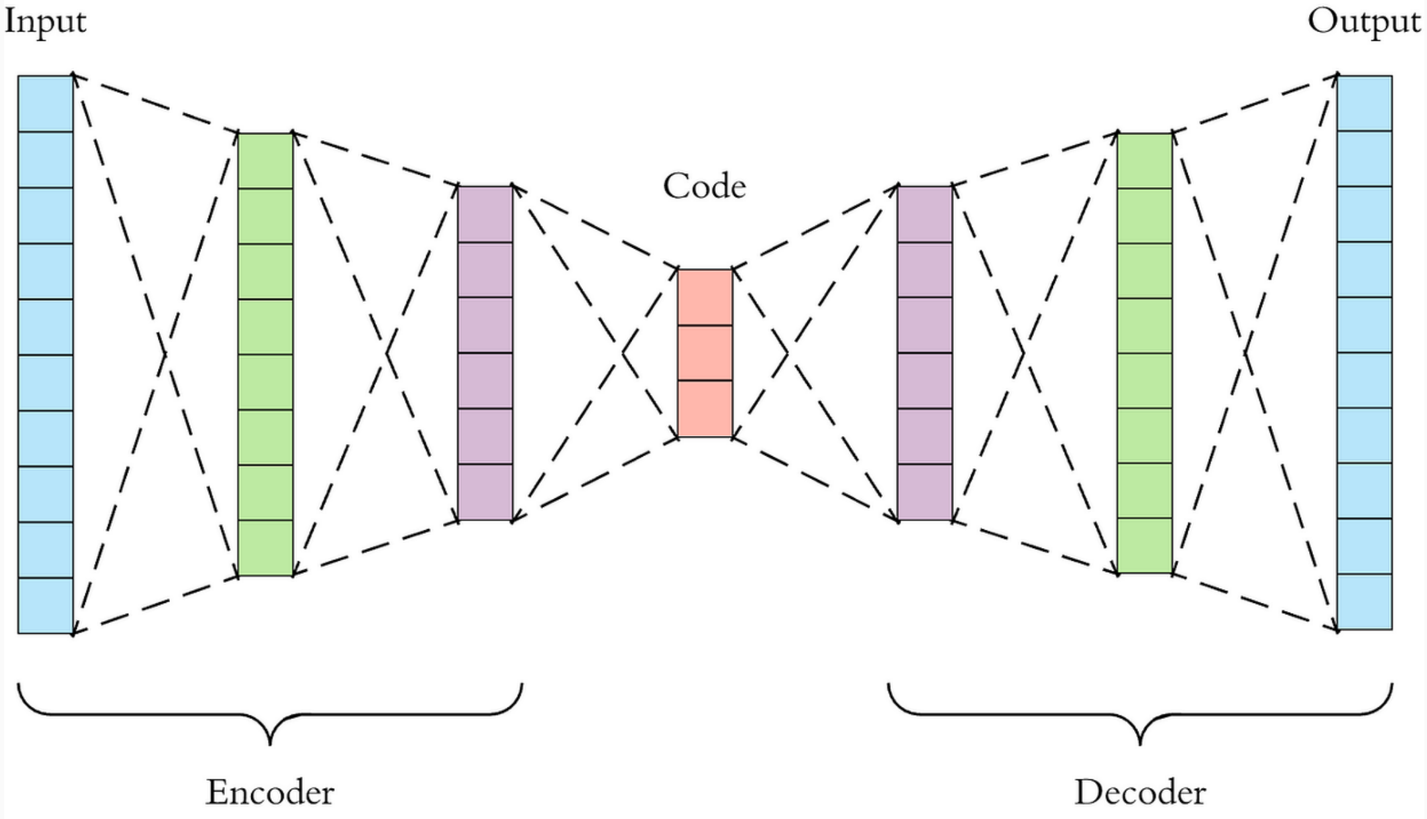
P(B | M)	B	M
0.7	yes	h
0.3	no	h
0.1	yes	l
0.9	no	l

P(M | A,T)	M	A	T
0.1	h	n	a1
0.6	h	m	a1
0.7	h	o	a1
0.9	l	n	a1
0.4	l	m	a1
0.3	l	o	a1
0.2	h	n	a2
0.7	h	m	a2
0.9	h	o	a2
0.8	l	n	a2
0.3	l	m	a2
0.1	l	o	a2





Lumberjack is going Deep!



Decoding accuracy measured with the root mean standard/squared absolute error (R M S E , M A E 2)

Thank you for your attention!

Any questions?