Hybrid Vigor: Improving Detection by Combining ML with Extracted IOCs

Justin D. Whitaker
justin@whitaker.pro

September 13, 2024

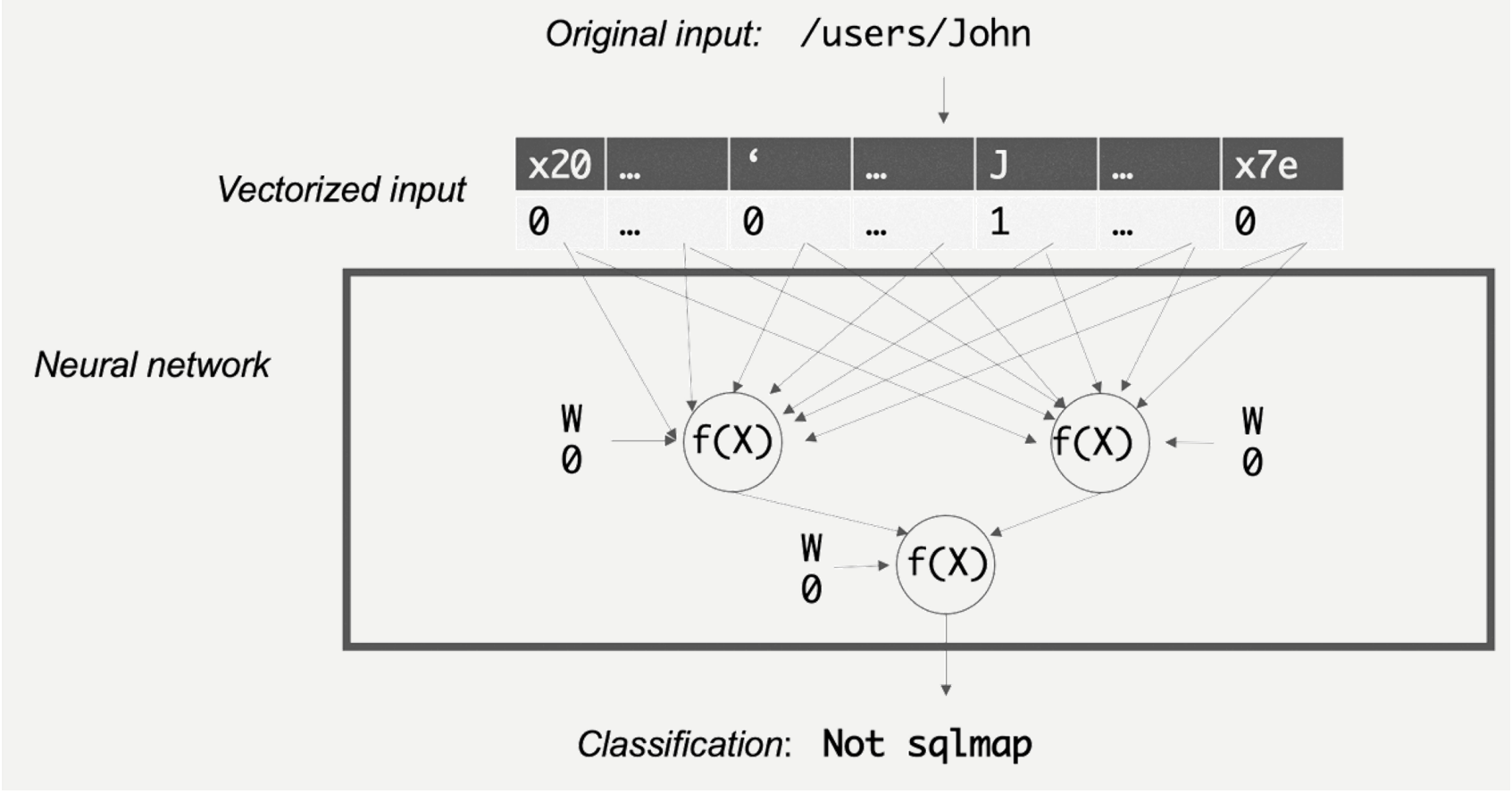
Background & Research Question

- My background
- Research question: is ML better than IOCs?

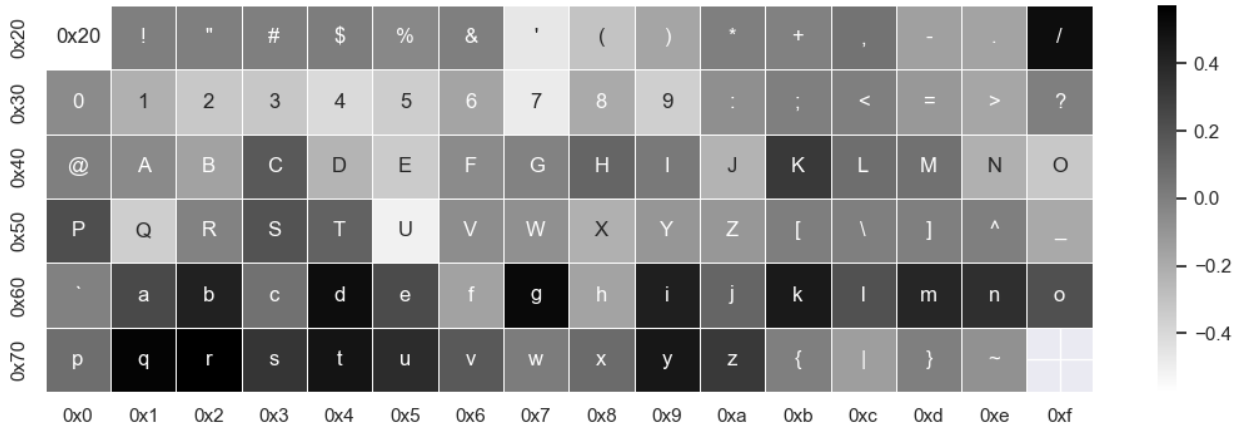
Creating a Dataset

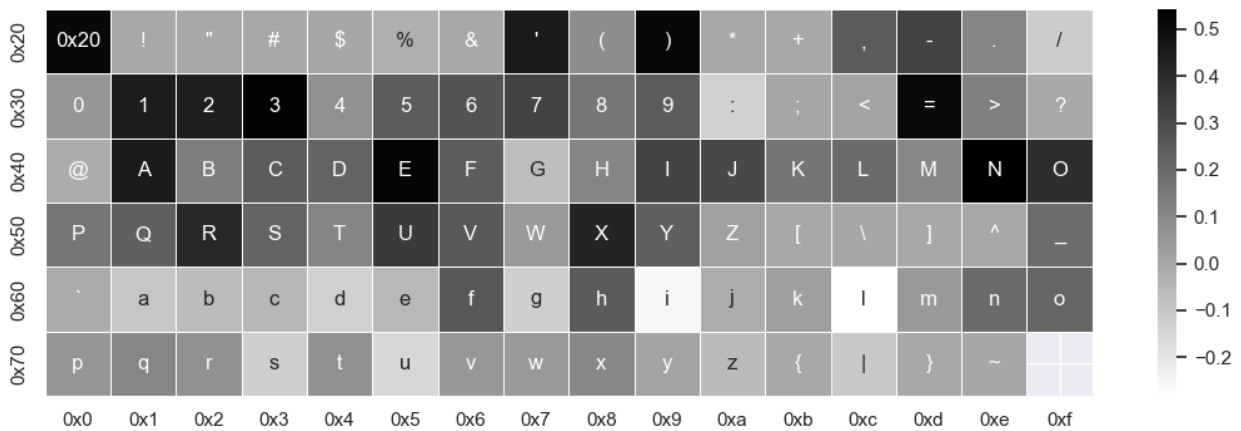
Dataset	Normal request	sqlmap request
1	/query/Alice	/query/John
	/query/Bob	/query/2005
	/query/Charlotte	/query/John.,(‘”(((,)
	/query/David	/query/John’ffyenR<’”>kXJw1Q
	/query/Ellie	/query/John) AND 8438=7839 AND (1986=1986
2	/query/1	/query/1
	/query/2	/query/8971
	/query/3	/query/1,'.")((.(.
	/query/4	/query/1,'.")((.(.
	/query/5	/query/1%2C%27.%22%29%28%28.%28.

Neural Network Architecture

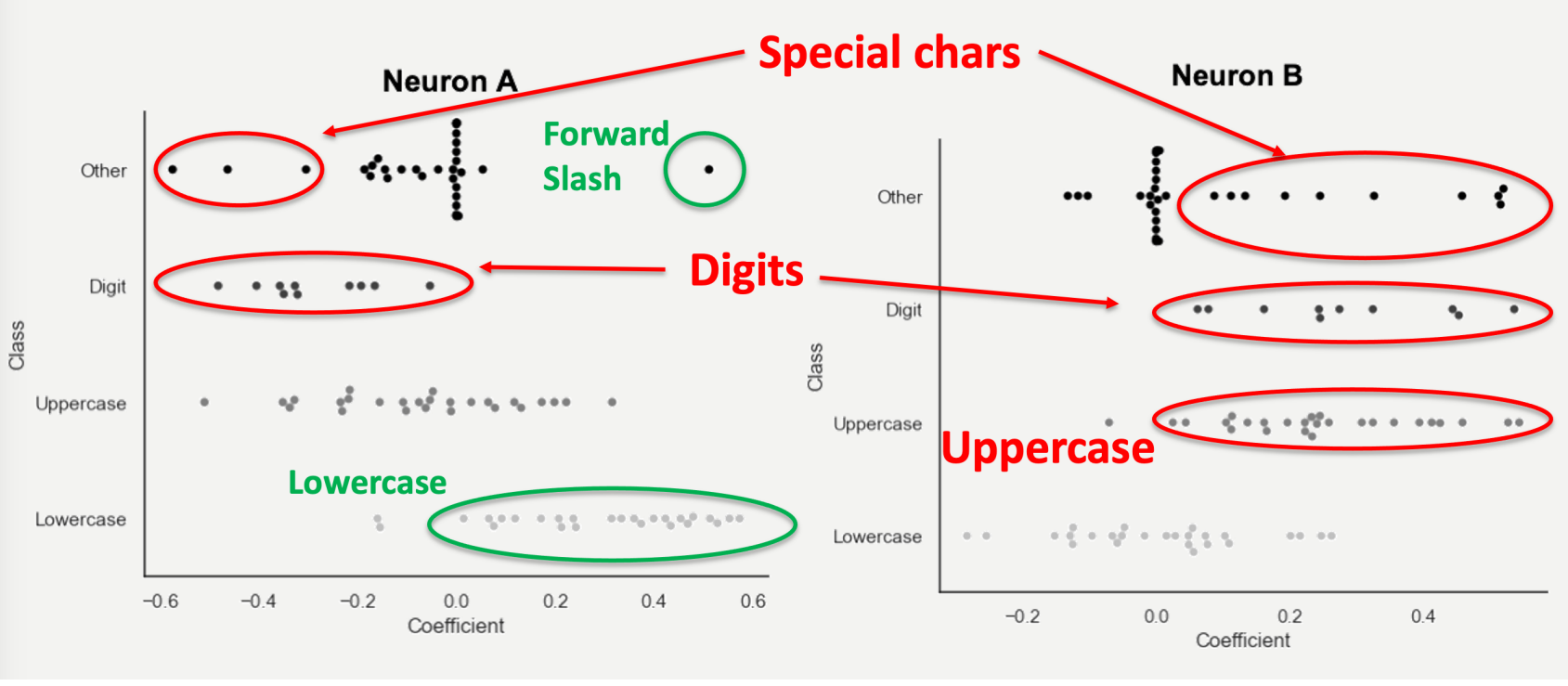


Neuron Coefficients

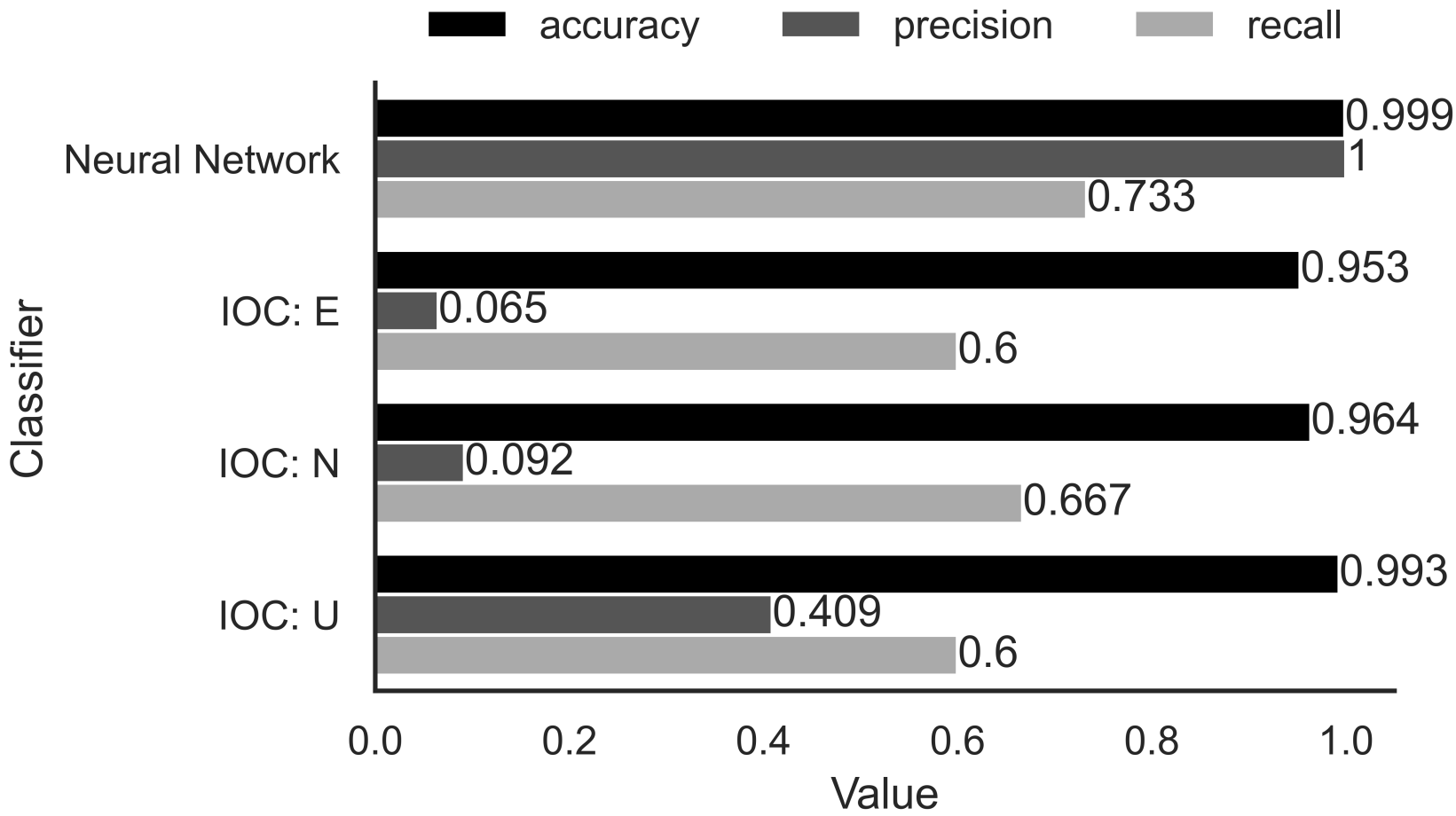




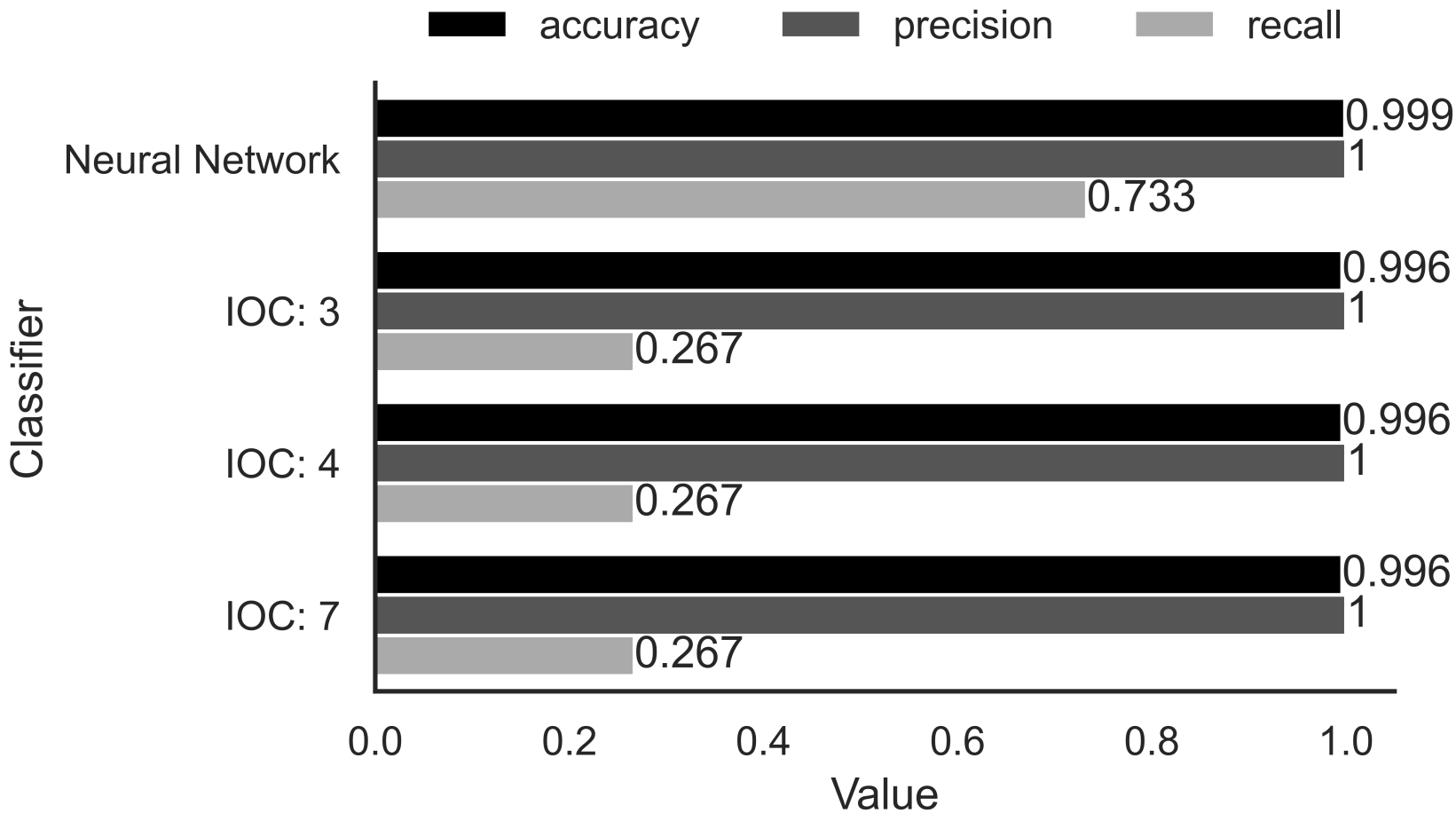
Neuron Coefficients: Another look



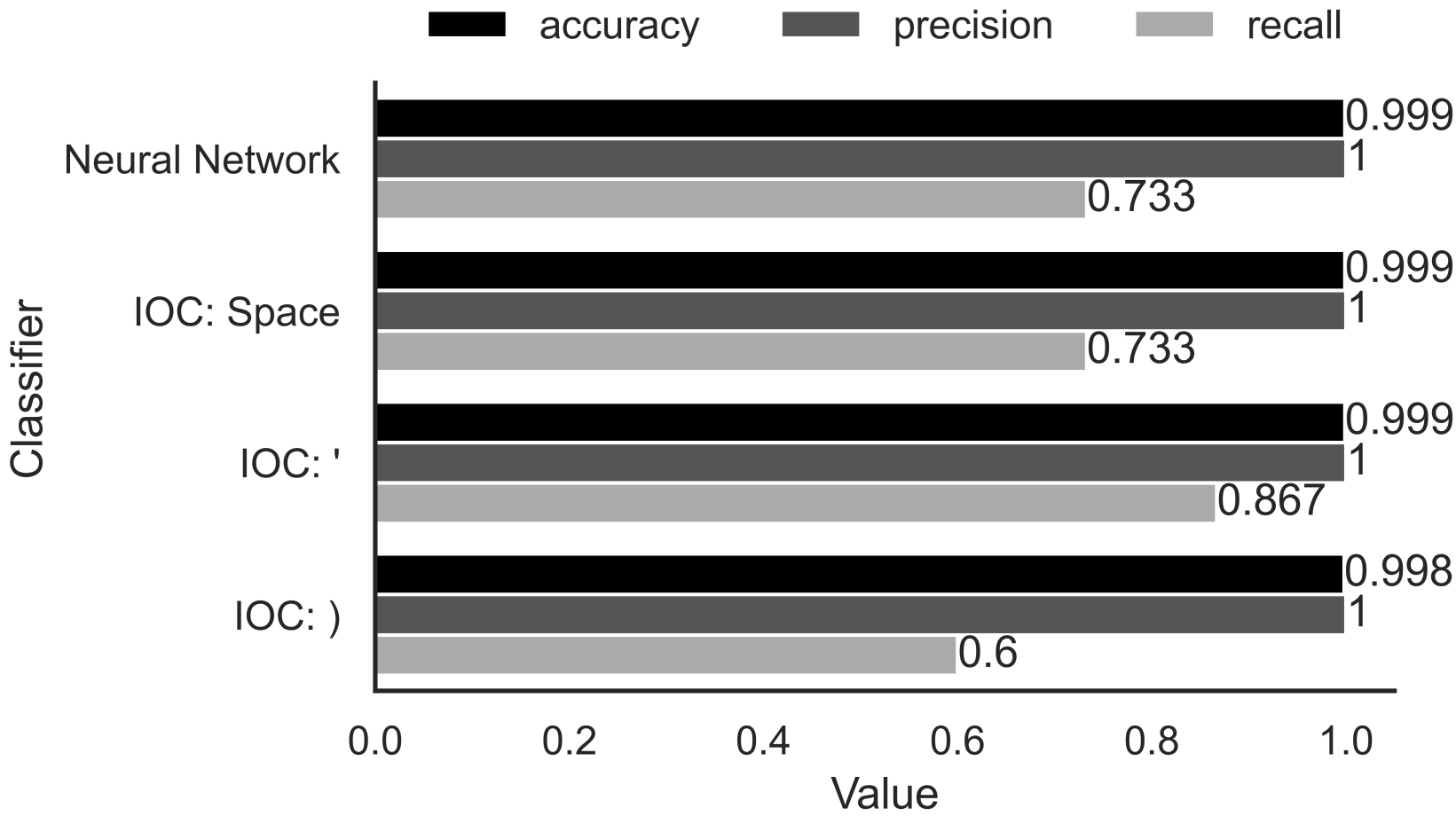
IOC: Uppercase Letters



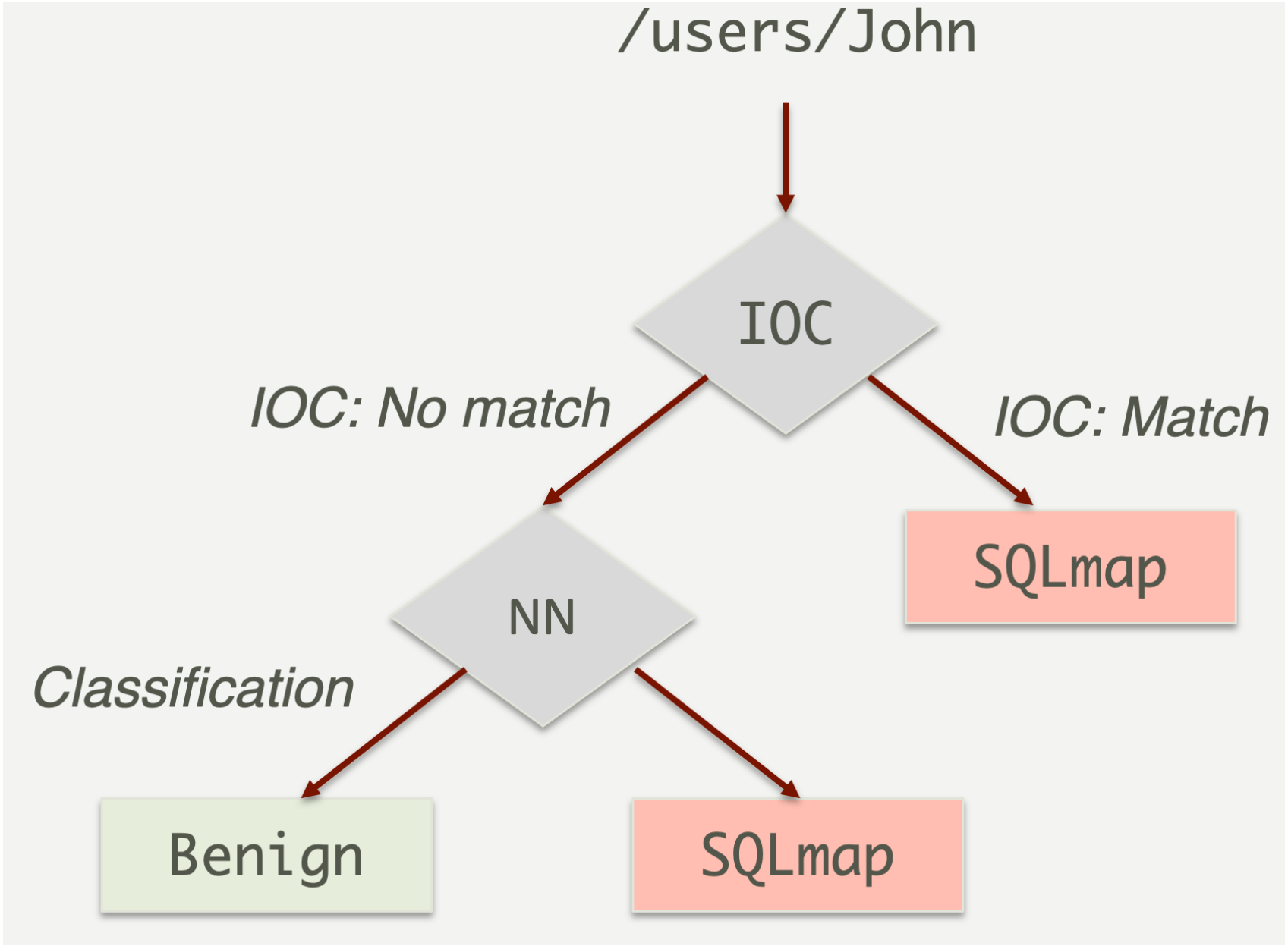
IOC: Digits


accuracy
precision
recall
Neural Network
IOC: 3
IOC: 4
IOC: 7
Classifier
0.999
1
0.733
0.996
1
0.267
0.996
1
0.267
0.996
1
0.267
0.0
0.2
0.4
0.6
0.8
1.0
Value

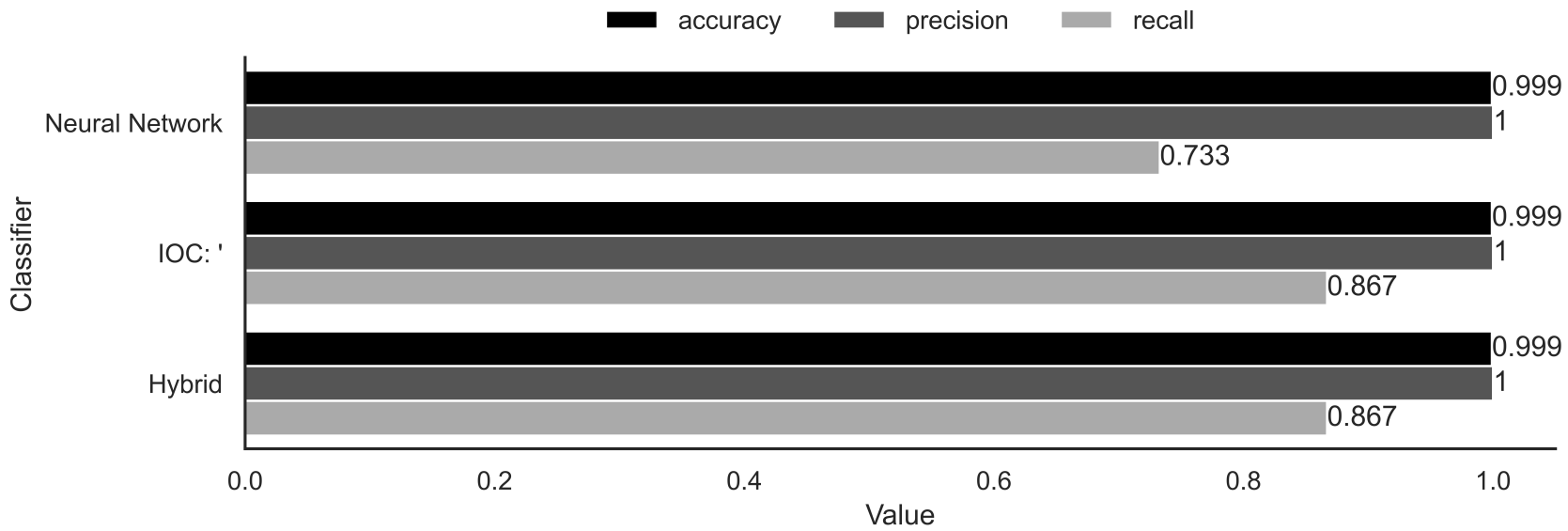
IOC: Special Characters



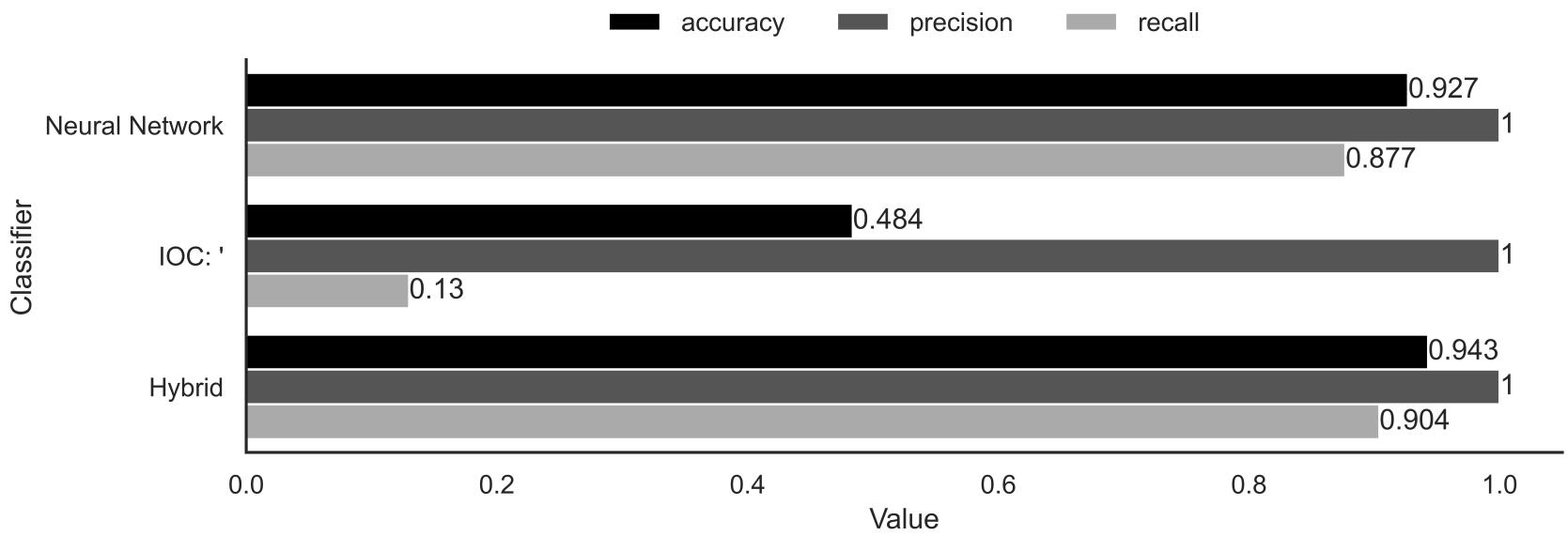
Hybrid Classifier Architecture



Performance: IOC wins!



Performance: Another Look



Takeaways

- We found that accuracy alone is not a sufficient metric to evaluate classifiers that detect attacks. Rather, more granular metrics such as recall and precision must be considered.
- We found that neural networks can mine data to discover highly effective IOCs.
- Neural networks generalize better to novel attack variants than IOCs.
- Hybrid classifiers that combine IOCs and machine learning can outperform both IOCs and machine learning alone.
- The code for this researcis available online at `https://github.com/jdwhitaker/hybrid-vigor`