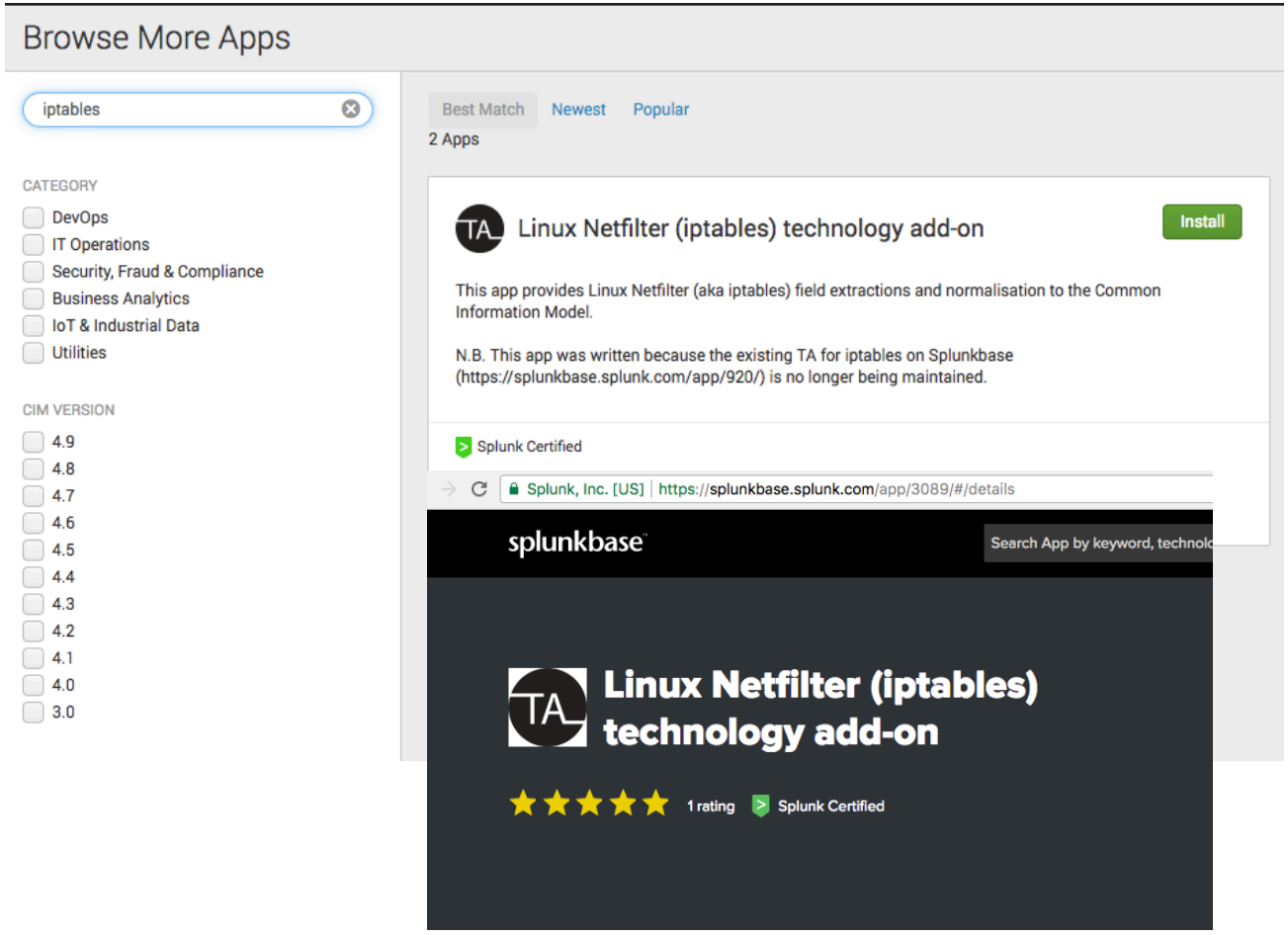
Apps to the Rescue



VERSION
0.1.2

BUILT BY
Doug Brown

CATEGORY & CONTENTS
Categories: Security, Fraud & Compliance
App Type: Add-on

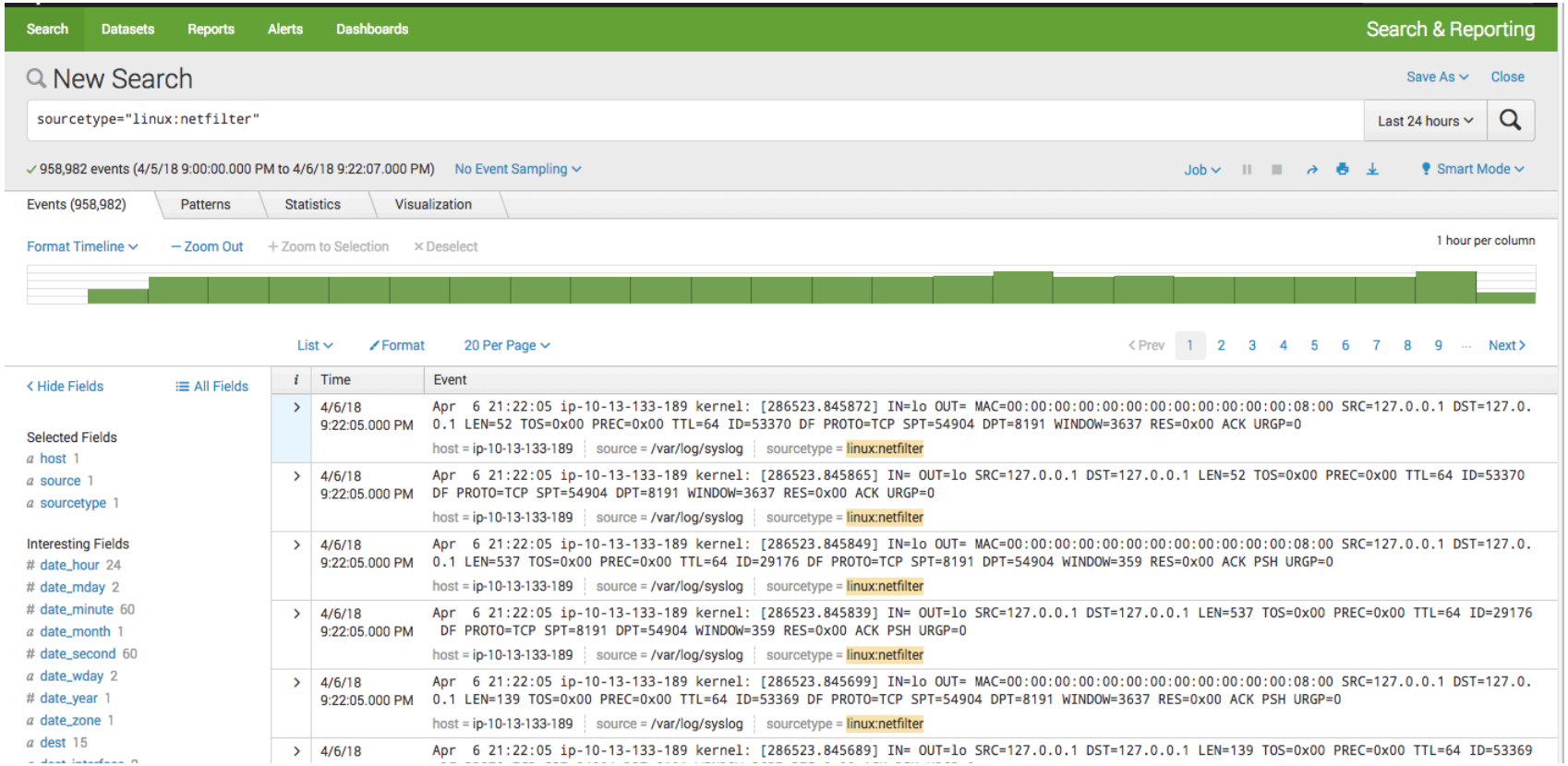
COMPATIBILITY
Products: Splunk Cloud, Splunk Enterprise
Splunk Versions: 7.0, 6.6, 6.5, 6.4, 6.3, 6.2
Platform: Platform Independent
CIM Versions: 4.9, 4.8, 4.7, 4.6, 4.5, 4.4

LICENSING
MIT

SUPPORT
Contact Developer
Developer Supported
Questions on Splunk Answers
Flag as inappropriate

What Does the App Give Us?

- Note: the sourcetype changes to “linux:netfilter”



What Does the App Give Us? CIM