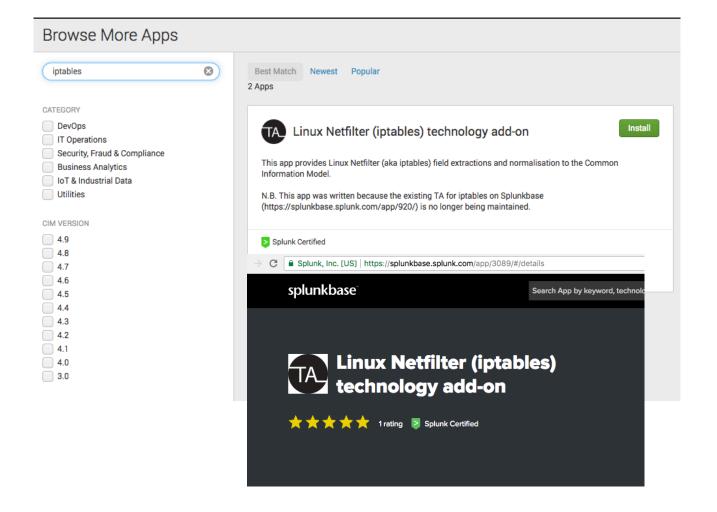


Apps to the Rescue



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

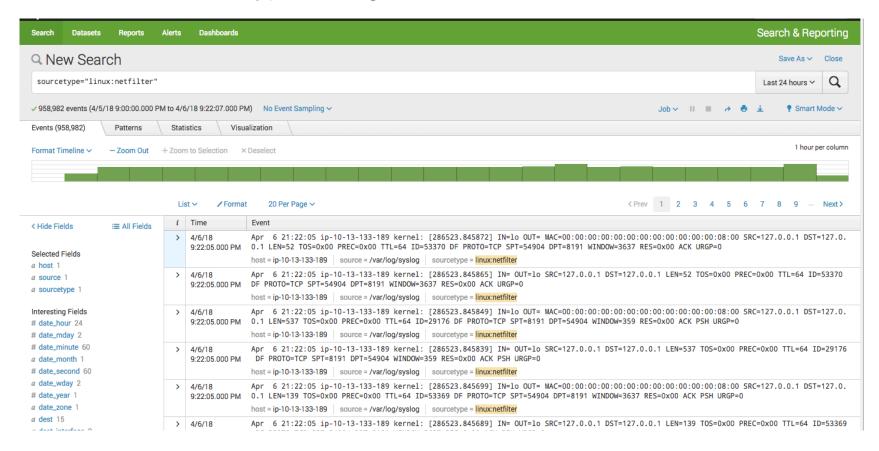
Questions on Splunk Answers

Flag as inappropriate



What Does the App Give Us?

Note: the sourcetype changes to "linux:netfilter"





What Does the App Give Us? CIM

linux_scripted_input (check report)

nix-all-logs nix_kernel_attached

127.0.0.1

protocol v

9:22:05.000 PM 0.1 LEN=52 TOS=0x00 PREC=0x00 TTL=64 ID=53370 DF PROT0=TCP SPT=54904 DPT=8191 WINDOW=3637 RES=0x00 ACK URGP=0 Event Actions > ✓ Field ■ SIC Y 127.0.0.1 Actions Selected ✓ host ✓ ip-10-13-133-189 src_interface v /var/log/syslog src_ip v 127.0.0.1 ✓ sourcetype ✓ linux:netfilter src_mac v 00:00:00:00:00:00 DPT ~ 8191 54904 src_port v DST V 127.0.0.1 FLAGS V ACK ☐ tag ∨ check FRAME_TYPE > 08:00 communicate 53370 network LEN V 52 report MAC ~ tcp_flag ~ ACK PREC ~ 0x00 tos v 0x00 TCP PROTO V transport > tcp RES ~ 0x00 SPT V 54904 64 127.0.0.1 vendor_product > Linux Netfilter TOS V OxOO 2018-04-06T21:22:05.000+00:00 Time 0 _time ~ TTLV Default index ~ URGP V WINDOW ~ 3637 linecount ∨ 127.0.0.1 dest v punct ~ __:_-:_-:[:]_=_=_=:::::::: dest_ip v 127.0.0.1 splunk_server > ip-10-13-133-189 dest_mac v 00:00:00:00:00:00 dest_port v 8191 Anr 6 21:22:05 in-10-13-133-189 kernel: [286523 845865] TN= OUT=lo SPC=127 O 0 1 D9 direction ~ inbound dvc v ip-10-13-133-189 dvc_host v eventtype > linux_netfilter (communicate network)