

Issues

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
6416	Suricata	Optimization	New	Normal	Suricata not using Myricom SNF driver in a performant way	Community Ticket	08/21/2025 02:00 PM
7062	Suricata	Feature	New	Normal	redis: support authenticating against a redis server	Community Ticket	08/04/2025 05:13 AM
2296	Suricata	Bug	Feedback	Normal	Unix Manager Should Not Use Conf Functions to Pass Information to source-pcap-file	Community Ticket	07/16/2025 07:22 PM
3873	Suricata	Bug	New	Normal	NET_RAW capability dropped for NFQ mode when uid/gid is specified	Community Ticket	07/16/2025 06:50 PM
3358	Suricata	Bug	Feedback	Normal	bypass_filter AFPBypassCallback Segmentation Fault	Community Ticket	07/16/2025 01:53 PM
6275	Suricata	Bug	New	Normal	fail af_xdp at configure time when libxdp is missing?	Community Ticket	07/16/2025 01:53 PM
3986	Suricata	Bug	New	Normal	suricata -r not working for sshfs-mounted folder but working for sshfs-mounted file	Community Ticket	07/16/2025 01:52 PM
3800	Suricata	Bug	New	Normal	Netronome XDP mode: Unable to find 'cpus_count' map"	Community Ticket	07/16/2025 01:40 PM
4214	Suricata	Bug	New	Normal	Honor vlan: use-for-tracking in ebpf maps	Community Ticket	07/16/2025 08:17 AM
2918	Suricata	Documentation	New	Normal	Unable to mmap, error Resource temporarily unavailable - err seems OS specific	Community Ticket	07/16/2025 08:13 AM
4183	Suricata	Bug	Feedback	Normal	Timestamps sometimes off by 2 hours on Windows	Community Ticket	07/16/2025 08:11 AM
3698	Suricata	Bug	New	Normal	Incorrect max length of windivert filter	Community Ticket	07/16/2025 08:10 AM
4740	Suricata	Bug	Feedback	Normal	libnet error with reject action on pfSense	Community Ticket	07/16/2025 08:09 AM
4186	Suricata	Bug	Feedback	Normal	error when cpu cores > 64 (use pf-ring)	Community Ticket	07/16/2025 08:08 AM
3801	Suricata	Bug	New	Normal	Problem hardware bypassing with Netronome	Community Ticket	07/16/2025 08:07 AM
1918	Suricata	Bug	New	Normal	Incorrect packet stats in pcap and pf_ring capture modes	Community Ticket	07/16/2025 08:00 AM
868	Suricata	Bug	New	Normal	Makefile[.in] doesn't use its own INSTALL variable definition	Community Ticket	07/16/2025 07:52 AM
4426	Suricata	Bug	Feedback	Normal	XDP redirect cpu likely broken in 5.9	Community Ticket	07/16/2025 07:50 AM
4357	Suricata	Bug	Feedback	Normal	Napatech memory corruption	Community Ticket	07/15/2025 03:31 PM
4016	Suricata	Bug	Feedback	Normal	filesize with filestore store empty files	Community Ticket	07/15/2025 12:41 PM
3353	Suricata	Bug	Feedback	Normal	xdp_filter segmentation fault util-ebpf.c:728	Community Ticket	07/15/2025 12:39 PM
4845	Suricata	Feature	New	Normal	IPv6 evasion : parasite6 + dos new ipv6 + fake mldrouter6 advertise	Community Ticket	07/15/2025 08:03 AM
1770	Suricata	Optimization	Feedback	Normal	Suricata takes very long time to start using hyperscan and large/custom detect settings	Community Ticket	07/11/2025 02:46 PM
3258	Suricata	Bug	Feedback	Normal	VXLAN exceeds MTU maximum	Community Ticket	07/11/2025 08:58 AM
6583	Suricata	Optimization	New	Normal	rust: get rid of unused final zeroes in protocol detection patterns	Community Ticket	07/09/2025 08:47 PM
1370	Suricata	Feature	New	Normal	sctp fp on suricata engine	Community Ticket	07/09/2025 02:19 PM
1819	Suricata	Feature	New	Normal	Silent installer for suricata windows	Community Ticket	06/16/2025 06:13 PM
2426	Suricata	Feature	New	Normal	tls: extend logging	Community Ticket	05/20/2025 12:35 PM
4286	Suricata	Bug	Feedback	Normal	FN occurs when using negated isdataat with http_cookie keyword	Community Ticket	03/05/2025 11:28 AM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
2858	Suricata	Feature	New	Normal	app-layer-protocol:failed; doesn't match traffic with ALPROTO_UNKNOWN	Community Ticket	03/05/2025 11:25 AM
4946	Suricata	Feature	New	Normal	nfsv2: implement WRITE support	Community Ticket	02/26/2025 08:55 AM
6572	Suricata	Optimization	New	Normal	runmodes: fix `--list-runmodes` output	Community Ticket	02/26/2025 08:45 AM
5711	Suricata	Bug	New	Normal	runmodes: Suricata does not hint anything about missing runmode	Community Ticket	02/26/2025 08:44 AM
1956	Suricata	Feature	New	Normal	Add option to re-initialise Lua output scripts	Community Ticket	02/11/2025 10:54 PM
7543	Suricata-Update	Task	New	Normal	windows: Install or document install a Python runtime	Community Ticket	02/04/2025 03:46 PM
3965	Suricata-Update	Task	New	Normal	windows: Support Suricata Update on Windows	Community Ticket	02/04/2025 03:46 PM
7542	Suricata-Update	Task	New	Normal	windows: file locations for configuration, rule files etc	Community Ticket	02/04/2025 03:43 PM
3734	Suricata	Optimization	New	Normal	af-packet: better support for csum offload	Community Ticket	01/09/2025 02:17 PM
4252	Suricata	Task	New	Normal	SCTP: session tracking	Community Ticket	11/19/2024 09:33 AM
2814	Suricata	Bug	New	Normal	suricatasc: hangs indefinitely and uses too much processing for pcap-file-continuos command	Community Ticket	11/12/2024 04:04 PM
2262	Suricata	Feature	Assigned	Normal	Unix Socket Output Configurable Retries and Blocking	Community Ticket	11/12/2024 04:04 PM
2975	Suricata	Task	Assigned	Normal	convert unittests to new FAIL/PASS API	Community Ticket	10/24/2024 07:07 PM
4911	Suricata	Task	New	Normal	tracking: detect: cleanup tests	Community Ticket	10/23/2024 09:54 PM
7342	Suricata	Optimization	New	Normal	aplayer/http: convert complex unittests to SV ones	Community Ticket	10/23/2024 09:35 PM
5030	Suricata	Documentation	New	Normal	Documentation bugs for endswith, distance, within	Community Ticket	10/16/2024 06:02 PM
6340	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/detect-http-method.c	Community Ticket	10/08/2024 09:03 AM
6358	Suricata	Task	Assigned	Normal	detect/analyzer: add more details for the ICMP itype keyword	Community Ticket	10/07/2024 01:14 PM
7283	Suricata	Feature	New	Normal	installing suricatasc functionality without installing suricata entirely	Community Ticket	10/06/2024 06:33 AM
7298	Suricata	Documentation	New	Normal	schema/netflow: add missing field	Community Ticket	10/02/2024 07:47 PM
7299	Suricata	Documentation	New	Normal	eve/schema: document tls	Community Ticket	10/02/2024 07:42 PM
6694	Suricata	Documentation	New	Normal	placement of bitmask note about right shift behavior	Community Ticket	09/24/2024 08:29 PM
5583	Suricata	Optimization	New	Normal	output: iface shortening more compact	Community Ticket	09/24/2024 03:58 PM
6142	Suricata	Optimization	New	Normal	detect/lua: convert convoluted unittests to suricata-verify ones	Community Ticket	09/22/2024 04:51 PM
7244	Suricata	Documentation	New	Normal	userguide: explain multi-tenant default config	Community Ticket	09/06/2024 08:05 PM
6410	Suricata	Feature	New	Normal	Log packets/bytes per second in Suricata stats	Community Ticket	09/06/2024 02:32 PM
6330	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/stream-tcp-list.c	Community Ticket	09/06/2024 02:32 PM
3762	Suricata	Documentation	New	Normal	update documentation for user modes	Community Ticket	09/06/2024 02:31 PM
2772	Suricata	Feature	New	Normal	Add MPLS labels to alert output	Community Ticket	09/06/2024 02:21 PM
1892	Suricata	Documentation	New	Normal	rule docs should include example rules	Community Ticket	08/28/2024 12:57 PM
7222	Suricata	Documentation	New	Normal	userguide: document decoder events	Community Ticket	08/27/2024 01:01 PM
6406	Suricata	Documentation	New	Normal	userguide: remove ambiguous "we" usages	Community Ticket	08/26/2024 07:38 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
7220	Suricata	Documentation	New	Normal	guides: add a post on using 'ip' and 'tcpdump' to Suricata forum's Guides	Community Ticket	08/23/2024 05:38 PM
4070	Suricata	Feature	New	Normal	capture plugins: receive notification when suricata is done with a packet	Community Ticket	07/09/2024 12:25 PM
3299	Suricata	Task	New	Normal	tracking: Add support for industrial protocol	Community Ticket	06/26/2024 08:13 AM
3300	Suricata	Task	New	Normal	tracking: Add support for medical protocols	Community Ticket	06/26/2024 08:12 AM
3289	Suricata-Update	Feature	Assigned	Normal	option to verify 'better' standard/schema	Community Ticket	06/21/2024 03:41 PM
4755	Suricata	Bug	New	Normal	eve: timestamp loses sub-second precision in some arm scenarios	Community Ticket	06/21/2024 03:34 PM
4087	Suricata	Bug	New	Normal	excessive CPU usage on Windows with --pcap-file-continuous option	Community Ticket	06/21/2024 03:31 PM
4841	Suricata	Task	New	Normal	tracking: research evasions wrt malformed IP and TCP options	Community Ticket	06/21/2024 03:25 PM
4770	Suricata	Feature	New	Normal	eve: specialized output for ML on packet sizes and similar properties	Community Ticket	06/21/2024 03:23 PM
4559	Suricata	Feature	New	Normal	Tags for rules that enables mapping to Mitre Att&ck	Community Ticket	06/21/2024 03:18 PM
4758	Suricata	Feature	Feedback	Normal	dns: weird query should have app-layer-event?	Community Ticket	06/21/2024 03:12 PM
4333	Suricata	Feature	New	Normal	Include the 'short name' from classification.config in the all-eve.log	Community Ticket	06/21/2024 03:09 PM
4270	Suricata	Feature	New	Normal	load rules from database	Community Ticket	06/21/2024 03:08 PM
4251	Suricata	Task	New	Normal	protocol: SCTP support	Community Ticket	06/21/2024 03:08 PM
4179	Suricata	Feature	New	Normal	tunnel-Node for flow, netflow and dns-events in eve.json	Community Ticket	06/21/2024 03:04 PM
3960	Suricata	Feature	New	Normal	Python tool to simulate GAP testing	Community Ticket	06/21/2024 02:59 PM
3959	Suricata	Feature	New	Normal	Python tool to take ip rules and convert into iprep rule(s)	Community Ticket	06/21/2024 02:58 PM
3950	Suricata	Feature	New	Normal	Suricata bash completion	Community Ticket	06/21/2024 02:58 PM
3848	Suricata	Feature	Feedback	Normal	Keep a Reference to Matched Items in Suricata Datasets for Rule-Writing	Community Ticket	06/21/2024 02:57 PM
3875	Suricata	Feature	New	Normal	Support multiple XFF	Community Ticket	06/21/2024 02:52 PM
3849	Suricata	Feature	New	Normal	Extend Suricata Datasets to Datamaps with Keys and Values	Community Ticket	06/21/2024 02:51 PM
3845	Suricata	Feature	New	Normal	Threshold Hit Counter (for SID/IP)	Community Ticket	06/21/2024 02:49 PM
3454	Suricata	Feature	New	Normal	Add support to communicate with other networking products	Community Ticket	06/21/2024 02:33 PM
6361	Suricata	Documentation	New	Normal	userguide: add note about severity<-> priority on alert section	Community Ticket	06/18/2024 02:02 PM
6311	Suricata	Task	New	Normal	detect/analyzer: add more details for the flowint keyword	Community Ticket	06/18/2024 02:02 PM
6310	Suricata	Task	New	Normal	detect/analyzer: add more details for the ttl keyword	Community Ticket	06/18/2024 02:02 PM
5842	Suricata	Documentation	New	Normal	userguide: bring session about Suricata installation from Ubuntu PPA	Community Ticket	06/18/2024 02:02 PM
5801	Suricata	Optimization	New	Normal	filemagic keywords: increase code coverage and update documentation (if need be)	Community Ticket	06/18/2024 02:02 PM
5785	Suricata	Optimization	New	Normal	smb: use u32.to_be_bytes to replace function u32_as_bytes	Community Ticket	06/18/2024 02:02 PM
5545	Suricata	Optimization	New	Normal	prefilter keyword: increase code coverage	Community Ticket	06/18/2024 02:02 PM
5068	Suricata	Documentation	New	Normal	nfs: document rule keyword	Community Ticket	06/18/2024 02:02 PM
3748	Suricata	Documentation	New	Normal	Add documentation for flags keyword	Community Ticket	06/18/2024 02:02 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
4706	Suricata	Documentation	New	Normal	Guide for rulewriting	Community Ticket	06/18/2024 02:02 PM
4217	Suricata	Feature	New	Normal	not complete cmd start line does not produce expliccit enough warning or msg	Community Ticket	06/18/2024 02:02 PM
3953	Suricata	Feature	New	Normal	8021BR E packet decoder	Community Ticket	06/18/2024 02:02 PM
4023	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API: detect-engine-address-ipv6.c	Community Ticket	06/18/2024 02:02 PM
4022	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-engine-address-ipv4.c	Community Ticket	06/18/2024 02:02 PM
6325	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-urilen.c	Community Ticket	06/18/2024 01:36 PM
6324	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - stream-tcp-reassemble.c	Community Ticket	06/18/2024 01:36 PM
6323	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - ippair-bit.c	Community Ticket	06/18/2024 01:36 PM
6322	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - util-pool.c	Community Ticket	06/18/2024 01:36 PM
6321	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - decode-raw.c	Community Ticket	06/18/2024 01:36 PM
6320	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-base64-data.c	Community Ticket	06/18/2024 01:36 PM
6319	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - util-bloomfilter.c	Community Ticket	06/18/2024 01:36 PM
6317	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-filestore.c	Community Ticket	06/18/2024 01:36 PM
6316	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - app-layer-detect-proto.c	Community Ticket	06/18/2024 01:36 PM
6315	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - ippair-storage.c	Community Ticket	06/18/2024 01:36 PM
6314	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/detect-http-client-body.c	Community Ticket	06/18/2024 01:36 PM
6356	Suricata	Task	New	Normal	detect/analyzer: add more details for the tcp.hdr keyword	Community Ticket	06/18/2024 01:35 PM
6351	Suricata	Task	New	Normal	detect/analyzer: add more details for the xbits keyword	Community Ticket	06/18/2024 01:35 PM
6350	Suricata	Task	New	Normal	detect/analyzer: add more details for the tcp.flags keyword	Community Ticket	06/18/2024 01:35 PM
6346	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-engine-dcepayload.c	Community Ticket	06/18/2024 01:35 PM
6344	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - detect-pcre.c	Community Ticket	06/18/2024 01:35 PM
6343	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/stream-tcp.c	Community Ticket	06/18/2024 01:35 PM
6341	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - decode-ethernet.c	Community Ticket	06/18/2024 01:35 PM
6338	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/detect-http-stat-msg.c	Community Ticket	06/18/2024 01:35 PM
6336	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - tests/detect-http-stat-code.c	Community Ticket	06/18/2024 01:35 PM
6335	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - decode-tcp.c	Community Ticket	06/18/2024 01:35 PM
6334	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - util-spm.c	Community Ticket	06/18/2024 01:35 PM
6333	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - util-rule-vars.c	Community Ticket	06/18/2024 01:35 PM
6331	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - util-bloomfilter-counting.c	Community Ticket	06/18/2024 01:35 PM
6327	Suricata	Task	New	Normal	Convert unittests to new FAIL/PASS API - threads.c	Community Ticket	06/18/2024 01:35 PM
6200	Suricata	Feature	New	Normal	output: suricata.yaml dump-all-headers applied for alerts	Community Ticket	06/14/2024 10:56 AM
5737	Suricata	Feature	New	Normal	smtp body extract	Community Ticket	06/11/2024 07:26 AM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
6461	Suricata	Feature	New	Normal	ics protocol: bacnet	Community Ticket	05/21/2024 08:33 PM
4951	Suricata	Feature	Assigned	Normal	decode: datalink type 276 not yet supported	Community Ticket	04/12/2024 09:12 AM
4372	Suricata	Documentation	New	Normal	Fix links in userguide	Community Ticket	11/22/2023 04:24 PM
4184	Suricata	Bug	New	Normal	createst: log fields introduced by debug mode should not be a part of test.yaml	Community Ticket	11/16/2023 05:22 AM
4268	Suricata	Feature	New	Normal	createst: allow to add options with --set	Community Ticket	11/16/2023 05:22 AM
6464	Suricata	Feature	New	Normal	protocol: profibus	Community Ticket	11/10/2023 09:07 AM
1950	Suricata	Feature	New	Normal	allow configuration of file-store types	Community Ticket	11/09/2023 02:07 PM
1899	Suricata	Feature	New	Normal	Detecting Malicious TCP Network Flows Based on Benford's Law	Community Ticket	11/09/2023 02:03 PM
4148	Suricata	Feature	New	Normal	Research: SSH Support for additional protocol analysis	Community Ticket	11/09/2023 11:04 AM
5670	Suricata	Feature	Feedback	Normal	Support wide strings somehow	Community Ticket	11/09/2023 10:32 AM
6462	Suricata	Feature	New	Normal	IEC104 Protocol Support	Community Ticket	11/09/2023 09:41 AM
4743	Suricata	Documentation	New	Normal	Improve Suricata code documentation (C files)	Community Ticket	10/31/2023 01:21 PM
547	Suricata	Feature	New	Normal	libinjection -- sqli library	Community Ticket	07/31/2023 10:07 PM
473	Suricata	Feature	New	Normal	pcap log: alert log with packet indexes	Community Ticket	07/21/2023 09:01 AM
936	Suricata	Feature	New	Normal	support tzsp protocol	Community Ticket	07/21/2023 08:37 AM
923	Suricata	Optimization	New	Normal	memcap value in suricata.yaml : erroring if config value is bigger than what is available	Community Ticket	07/21/2023 08:31 AM
821	Suricata	Feature	New	Normal	conditional logging: output steering	Community Ticket	07/21/2023 08:12 AM
808	Suricata	Optimization	Assigned	Normal	Support the new GSO-avoidance NFQ feature	Community Ticket	07/21/2023 08:04 AM
721	Suricata	Optimization	New	Normal	full nfq zero copy mode	Community Ticket	07/21/2023 08:03 AM
795	Suricata	Optimization	New	Normal	stream: use pool instead of direct SACK record allocs	Community Ticket	07/21/2023 07:59 AM
659	Suricata	Feature	New	Normal	Update IP reputation from unix socket.	Community Ticket	07/19/2023 08:09 PM
614	Suricata	Optimization	Assigned	Normal	Rate limiting messages	Community Ticket	07/19/2023 08:05 PM
266	Suricata	Feature	New	Normal	log http raw request for network forensic	Community Ticket	07/19/2023 07:59 PM
500	Suricata	Bug	New	Normal	duplicate values in host-os-policy not detected	Community Ticket	07/19/2023 07:56 PM
569	Suricata	Optimization	New	Normal	display syntax requirement on keyword parsing error	Community Ticket	07/19/2023 03:04 PM
6206	Suricata	Feature	New	Normal	Investigate a more intuitive use of the timestamp field in traffic/metadata events	Community Ticket	07/13/2023 03:22 PM
2627	Suricata	Bug	New	Normal	lua: load script from same location as rule file if not in default rule location	Community Ticket	06/30/2023 02:12 PM
4398	Suricata	Feature	New	Normal	support regex match and flowvars as keywords value	Community Ticket	06/30/2023 02:12 PM
4381	Suricata	Feature	New	Normal	flowbits: warn if flowbit dependencies don't follow suricata inspection order	Community Ticket	06/30/2023 02:12 PM
4547	Suricata	Feature	New	Normal	pcrexform not support tcp and other protocol	Community Ticket	06/30/2023 02:09 PM
3894	Suricata	Feature	New	Normal	Option "ttl" exclusive range behavior is non-intuitive	Community Ticket	06/30/2023 01:55 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
3829	Suricata	Optimization	New	Normal	pcap source: Counters, counters and... counters	Community Ticket	06/30/2023 07:53 AM
3830	Suricata	Optimization	New	Normal	pcap source: PcapThreadVars and cache lines	Community Ticket	06/30/2023 07:53 AM
5776	Suricata	Feature	New	Normal	PCRE fast_patterns via hyperscan	Community Ticket	06/09/2023 01:30 PM
4649	Suricata	Feature	New	Normal	Autonomous System Number (ASN) support similar to GeoIP	Community Ticket	06/09/2023 12:28 PM
2818	Suricata	Feature	New	Normal	Napatech Bypass support	Community Ticket	05/18/2023 01:00 PM
2701	Suricata	Feature	New	Normal	flow: counter for allocations at runtime	Community Ticket	05/18/2023 09:10 AM
2460	Suricata	Optimization	New	Normal	Reduce timeout in unix-socket when multiple pcaps are enqueued	Community Ticket	05/18/2023 09:09 AM
2107	Suricata	Feature	New	Normal	eve: rotate log output based on size	Community Ticket	05/18/2023 09:07 AM
4390	Suricata	Feature	New	Normal	Read pcap from standard in with "-r -"	Community Ticket	05/10/2023 01:36 PM
5913	Suricata	Feature	New	Normal	rfb: add more record types	Community Ticket	03/17/2023 09:27 AM
5872	Suricata	Feature	New	Normal	file structure awareness - precise identification of fields in file structs	Community Ticket	03/04/2023 09:46 AM
4864	Suricata	Task	New	Normal	Increase coverage of unit tests across Suricata	Community Ticket	02/14/2023 01:08 PM
5591	Suricata	Documentation	New	Normal	devguide: bring section about OpenBSD Installation from git into devguide	Community Ticket	02/01/2023 06:48 PM
3964	Suricata-Update	Bug	New	Normal	Windows: Fix failure due to file permission issues	Community Ticket	12/07/2022 08:36 PM
3201	Suricata	Bug	New	Normal	suricata-verify: Shell checks are not correctly addressed	Community Ticket	12/07/2022 04:30 PM
5680	Suricata	Optimization	New	Normal	eve-log: reduce duplication of info	Community Ticket	11/15/2022 05:51 AM
5678	Suricata	Task	New	Normal	tracking: Parse protocols that are not over TCP/UDP	Community Ticket	11/15/2022 05:47 AM
5675	Suricata	Feature	New	Normal	protocol: MMS SCADA support	Community Ticket	11/13/2022 08:47 AM
4662	Suricata	Documentation	New	Normal	Add documentation section covering Suricata rule grammar	Community Ticket	11/11/2022 01:19 PM
4325	Suricata	Feature	New	Normal	xdp compile warnings on 5.4 kernels	Community Ticket	10/27/2022 04:28 PM
3310	Suricata	Feature	New	Normal	ease suricata configuration with xdp	Community Ticket	10/27/2022 04:25 PM
3127	Suricata	Optimization	New	Normal	Unable to set XDP on 'ens2f0': Invalid argument (-22) - Mellanox cards and Intel cards with jumbo frames	Community Ticket	10/27/2022 04:24 PM
2613	Suricata	Feature	New	Normal	stats: add xdp counters to stats	Community Ticket	10/27/2022 04:24 PM
1954	Suricata	Feature	New	Normal	runtime option/flag to disable hardware timestamp support	Community Ticket	10/27/2022 04:24 PM
2269	Suricata	Feature	New	Normal	TLS: tls.version: allow negation or comparison	Community Ticket	10/27/2022 01:29 PM
5209	Suricata	Feature	New	Normal	Add "status" mode to Suricata's socket command interface	Community Ticket	03/30/2022 10:42 AM
4150	Suricata	Feature	New	Normal	Profiling mode: Ticks used to generate an alert available?	Community Ticket	02/01/2022 02:46 PM
4870	Suricata	Task	New	Normal	Clean up unit tests across Suricata	Community Ticket	12/04/2021 06:31 PM
2987	Suricata	Feature	New	Normal	Suggestions for new keywords (streambits)	Community Ticket	03/06/2021 08:06 AM
2780	Suricata	Optimization	New	Normal	Convert DNP3 from C to Rust	Community Ticket	02/25/2021 03:18 PM
432	Suricata	Feature	New	Normal	PCAP-NG support	Community Ticket	02/13/2021 09:31 AM
273	Suricata	Feature	New	Normal	IRC protocol detection support	Community Ticket	12/24/2020 07:06 AM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
4203	Suricata	Feature	New	Normal	createst: ability to create diff between a PR and master	Community Ticket	12/07/2020 10:02 AM
4175	Suricata	Feature	New	Normal	dcerpc: higher level logging	Community Ticket	11/23/2020 01:14 PM
4147	Suricata	Feature	Feedback	Normal	Map rules to MITRE ATT&CK	Community Ticket	11/19/2020 09:25 PM
4151	Suricata	Task	New	Normal	Research: New protocol support	Community Ticket	11/19/2020 09:22 PM
4149	Suricata	Feature	Feedback	Normal	Research: Dynamic datasets	Community Ticket	11/19/2020 09:15 PM
4146	Suricata	Task	New	Normal	Research: Hand off packet streams on alerts	Community Ticket	11/19/2020 09:10 PM
2513	Suricata	Feature	Feedback	Normal	Suricata read the SSLProxy header	Community Ticket	11/09/2020 12:14 PM
3296	Suricata	Feature	Feedback	Normal	Include in the fileinfo if it was a duplicate	Community Ticket	11/06/2020 04:17 PM
3192	Suricata	Feature	New	Normal	POC advice for adding support for	Community Ticket	09/05/2020 09:29 PM
3122	Suricata	Feature	Feedback	Normal	action missing in packet delivered in Bypass Callback	Community Ticket	09/05/2020 09:26 PM
1767	Suricata	Feature	New	Normal	Support DTLS protocol	Community Ticket	07/14/2020 01:34 PM
2673	Suricata	Feature	New	Normal	Split out DNS parser to be reusable	Community Ticket	04/22/2020 07:07 PM
2925	Suricata	Feature	New	Normal	Support for SPB encapsulation	Community Ticket	01/30/2020 01:32 PM
3244	Suricata	Feature	New	Normal	IMAP Support	Community Ticket	01/30/2020 11:55 AM
3305	Suricata	Optimization	New	Normal	Tracking ticket: which parts of the engine should be dynamic	Community Ticket	11/13/2019 09:08 AM
3295	Suricata	Feature	New	Normal	Unix socket: support to receive flow shunting information	Community Ticket	11/09/2019 01:09 PM
3316	Suricata	Feature	Feedback	Normal	Unix socket: support dumping flow table	Community Ticket	11/05/2019 09:21 PM
3291	Suricata	Task	Feedback	Normal	collect common mistakes rulewriters might run into	Community Ticket	11/05/2019 11:14 AM
3301	Suricata	Task	New	Normal	Research: Failover support within the current IPS implementation	Community Ticket	11/05/2019 10:51 AM
3302	Suricata	Task	New	Normal	Research: ruleset optimizations	Community Ticket	11/05/2019 10:51 AM
3246	Suricata	Feature	New	Normal	Logging of Email body	Community Ticket	10/20/2019 08:45 PM
3245	Suricata	Feature	New	Normal	Email extraction to separate folder	Community Ticket	10/20/2019 08:45 PM
3222	Suricata	Documentation	New	Normal	Configuring ipv6	Community Ticket	10/20/2019 08:43 PM
3212	Suricata	Feature	New	Normal	Prevent duplicate pcaps from being re-processed	Community Ticket	10/08/2019 01:53 AM
1749	Suricata	Optimization	New	Normal	Log PACKET_DROP in inline mode for invalid states as well	Community Ticket	10/01/2019 10:21 PM
1566	Suricata	Feature	New	Normal	ICMPv4 control channel detection	Community Ticket	09/27/2019 01:55 PM
1571	Suricata	Feature	New	Normal	Socket permissions setting in suricata.yaml	Community Ticket	09/27/2019 01:50 PM
1718	Suricata	Optimization	New	Normal	Time stamp in Log files should be ISO 8601 format	Community Ticket	09/27/2019 01:28 PM
1794	Suricata	Feature	New	Normal	test suricata rules over unix-socket	Community Ticket	09/27/2019 01:10 PM
2273	Suricata	Feature	Assigned	Normal	engine analysis: enable analysis by default during startup	Community Ticket	09/27/2019 08:40 AM
2410	Suricata	Feature	New	Normal	Create a reset counter and track maximum number of parallel flows	Community Ticket	09/27/2019 07:58 AM
2589	Suricata	Documentation	New	Normal	document decode-event	Community Ticket	09/25/2019 07:20 PM
1974	Suricata	Documentation	New	Normal	DNP3: document lua support	Community Ticket	09/25/2019 07:19 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
535	Suricata	Feature	New	Normal	new keywords - time , day	Community Ticket	06/30/2019 07:51 PM
1541	Suricata	Feature	New	Normal	multi-detect - vlan range mapping	Community Ticket	06/30/2019 06:46 PM
902	Suricata	Feature	Assigned	Normal	VLAN host table support	Community Ticket	05/31/2019 09:58 PM
2648	Suricata	Feature	New	Normal	store captured data into file	Community Ticket	05/23/2019 09:52 PM
2661	Suricata	Feature	New	Normal	output the http-body-data to eve.json	Community Ticket	05/23/2019 09:52 PM
2672	Suricata	Feature	New	Normal	Split out DHCP parser to be reusable	Community Ticket	05/23/2019 09:51 PM
2674	Suricata	Feature	New	Normal	Split out NFS parser to be reusable	Community Ticket	05/23/2019 09:51 PM
2767	Suricata	Feature	New	Normal	Interception of network stack attacks	Community Ticket	05/23/2019 09:43 PM
2935	Suricata	Feature	New	Normal	Support for multiple-logger for drop eve-log	Community Ticket	04/18/2019 11:41 AM
1741	Suricata	Feature	New	Normal	flow: use capture methods flow hash	Community Ticket	04/08/2019 12:12 PM
2759	Suricata	Feature	New	Normal	iprep: more granularity	Community Ticket	03/12/2019 11:44 AM
1995	Suricata	Feature	New	Normal	fast.log should show if packet has been dropped or rejected	Community Ticket	03/12/2019 11:01 AM
276	Suricata	Feature	New	Normal	Libcap support for dropping privileges	Community Ticket	03/11/2019 02:06 PM
2569	Suricata	Feature	New	Normal	multi-tenancy: allow mapping to 'device pair' in IPS mode	Community Ticket	03/11/2019 01:52 PM
2174	Suricata	Feature	New	Normal	Need a special keyword and functionality for ip address extraction from a content (html body for ex.) and comparing it to src,dst_ip/EXTERNAL,HOME_NET	Community Ticket	02/23/2019 10:20 PM
1799	Suricata	Feature	New	Normal	netmap: capture drop stats	Community Ticket	02/23/2019 10:18 PM
1783	Suricata	Feature	New	Normal	Create Suricata buffers to expose L2, L3, and L4 headers to Lua scripts	Community Ticket	02/23/2019 10:18 PM
1750	Suricata	Feature	New	Normal	Set Suricata to listen to all network interfaces when using AF_PACKET	Community Ticket	02/23/2019 10:18 PM
1712	Suricata	Feature	New	Normal	multitenancy: 'lite' tenants	Community Ticket	02/23/2019 10:17 PM
1710	Suricata	Feature	New	Normal	Unix socket: Send output to unix socket	Community Ticket	02/23/2019 10:17 PM
1590	Suricata	Feature	New	Normal	lua: force file magic and md5 lookup from script	Community Ticket	02/23/2019 10:17 PM
1489	Suricata	Feature	New	Normal	Log a message when memcap limit is reached	Community Ticket	02/23/2019 10:16 PM
1313	Suricata	Optimization	New	Normal	All Free functions should correctly handle NULL pointers	Community Ticket	02/23/2019 10:16 PM
1290	Suricata	Feature	New	Normal	handle SIGHUP signal	Community Ticket	02/23/2019 10:16 PM
1247	Suricata	Bug	New	Normal	Using suppress in threshold.config does not prevent dropping	Community Ticket	02/23/2019 10:15 PM
1234	Suricata	Feature	New	Normal	nfqueue: use mnl API	Community Ticket	02/23/2019 10:15 PM
1194	Suricata	Feature	New	Normal	Implement http_args keyword to match http arguments - query string or body	Community Ticket	02/23/2019 10:14 PM
1095	Suricata	Feature	New	Normal	Integration of support for STIX-based indicators	Community Ticket	02/23/2019 10:14 PM
1002	Suricata	Feature	New	Normal	Possible to disabling/bypassing a rule by a specific source ip and a destination ip?	Community Ticket	02/23/2019 10:13 PM
960	Suricata	Feature	New	Normal	persistent TCP resets	Community Ticket	02/23/2019 10:13 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
933	Suricata	Feature	New	Normal	add a IPv6 (RFC2460 recommended order of EH)rule to decoder events rules	Community Ticket	02/23/2019 10:13 PM
844	Suricata	Task	New	Normal	Testing topera against suricata	Community Ticket	02/23/2019 10:12 PM
728	Suricata	Feature	New	Normal	Add support for OpenCL	Community Ticket	02/23/2019 10:11 PM
716	Suricata	Feature	New	Normal	configurable packet_stats.csv and packet_stats.log	Community Ticket	02/23/2019 10:11 PM
682	Suricata	Feature	Assigned	Normal	Add DEP and ASLR to Windows Binary	Community Ticket	02/23/2019 10:11 PM
609	Suricata	Feature	New	Normal	Active Response in inline mode (like react in snort 2.9+)	Community Ticket	02/23/2019 10:10 PM
596	Suricata	Feature	New	Normal	rule profiling: multiple outputs per run	Community Ticket	02/23/2019 10:10 PM
536	Suricata	Optimization	New	Normal	share ctx for filemd5 keyword if identical files are used	Community Ticket	02/23/2019 10:09 PM
365	Suricata	Feature	New	Normal	expose interface(unix socket command) to reset tcp connection	Community Ticket	02/23/2019 10:08 PM
249	Suricata	Feature	New	Normal	Configure host-os-policy from a file, like snorts host_attribute.xml	Community Ticket	02/23/2019 10:07 PM
2227	Suricata	Feature	New	Normal	more detailed output about number of threads created	Community Ticket	02/23/2019 10:06 PM
2342	Suricata	Feature	New	Normal	Write PCAP files directly to Unix Socket	Community Ticket	02/23/2019 10:05 PM
2378	Suricata	Bug	New	Normal	log rotation 'flag' should be atomic	Community Ticket	02/23/2019 10:04 PM
2519	Suricata	Feature	New	Normal	XFF iprep support	Community Ticket	02/23/2019 10:03 PM
2538	Suricata	Feature	New	Normal	dsize keyword improvements	Community Ticket	02/23/2019 10:03 PM
1191	Suricata	Feature	New	Normal	EVE log does not support customformat	Community Ticket	02/23/2019 09:55 PM
3751	Suricata	Documentation	New	Low	Alert metadata JSON configs in suricata.yaml.in should match the RTD documentation	Community Ticket	09/25/2024 01:21 PM
3322	Suricata	Optimization	New	Low	Use standard CRC32 for hash-like functions	Community Ticket	09/23/2024 07:09 AM
4159	Suricata	Feature	New	Low	Log flow age as fractional value	Community Ticket	06/21/2024 03:01 PM
3797	Suricata	Optimization	New	Low	Filestore Setup Excess Directory Slash	Community Ticket	06/19/2024 08:55 AM
4083	Suricata	Optimization	In Progress	Low	Remove redundant code	Community Ticket	06/11/2024 07:17 AM
6824	Suricata	Documentation	New	Low	doc: Document every parameter of the configure script	Community Ticket	03/02/2024 01:59 PM
548	Suricata	Optimization	New	Low	Use bloomfilter for filemd5	Community Ticket	07/21/2023 09:01 AM
121	Suricata	Feature	New	Low	Alert on domain name look up, capture traffic for corresponding IP	Community Ticket	07/19/2023 02:10 PM
2880	Suricata-Update	Optimization	New	Low	Remove redundant code	Community Ticket	11/23/2022 05:53 PM
2310	Suricata	Feature	New	Low	lua: expose xbits	Community Ticket	03/06/2021 08:07 AM
3321	Suricata	Feature	New	Low	Evaluate different encoders for eve-log	Community Ticket	11/12/2020 12:51 PM
2976	Suricata	Documentation	Assigned	Low	review userguide from beginners point of view	Community Ticket	09/21/2020 02:33 PM
1216	Suricata	Feature	New	Low	Debian repository	Community Ticket	04/14/2020 10:09 PM
2687	Suricata	Optimization	New	Low	current suricata.yaml is missing rotate-interval "example"	Community Ticket	06/18/2019 08:40 PM
448	Suricata	Feature	New	Low	dlp: md5sum based on part of files	Community Ticket	03/11/2019 02:05 PM
1977	Suricata	Feature	New	Low	get the os info from TCP HTTP fingerprint	Community Ticket	02/23/2019 10:19 PM

#	Project	Tracker	Status	Priority	Subject	Assignee	Updated
1752	Suricata	Feature	New	Low	Netmap for Windows	Community Ticket	02/23/2019 10:18 PM
1215	Suricata	Feature	New	Low	journald logging support	Community Ticket	02/23/2019 10:15 PM
1188	Suricata	Optimization	New	Low	Don't use iface name in GetIfaceMaxHWHeaderLength	Community Ticket	02/23/2019 10:14 PM
949	Suricata	Feature	New	Low	SUSE automatic package building system	Community Ticket	02/23/2019 10:13 PM