# INDEX TABLE

Table 1: radio_frecuencia record fields ..... 2

Table 2: redes_moviles record fields ..... 2

Table 3: trafico_ids record fields ..... 3

Table 4: siem record fields ..... 4

Table 5: bluetooth record fields ..... 4

Table 6: wifi record fields ..... 5

Table 7: firewall record fields ..... 7

Table 8: ids_suricata ("fileinfo") record fields ..... 12

Table 9: ids_suricata ("flow") record fields ..... 13

Table 10: ids_suricata ("http") record fields ..... 15

Table 11: ids_suricata ("alert") record fields ..... 17

Table 12: ids_suricata ("stats") record fields ..... 20

# E. RECORDS

**Table 1: radio_frecuencia record fields**

| radio_frecuencia | |
|---|---|
| **Field** | **Example** |
| version | 1.0 |
| timestamp | 2021-02-25T11:30:21.000+0000 |
| id | f0c48ba4-387d-11ea-a137-2e728ce88126 |
| type | RF |
| event | DATA |
| signal | -62 |
| freq | 433.78 |
| mod | OOK |
| payload | 88e8e8e88888e8e888e8e8e800 |
| time | 2020-09-07T16:48:49.000+0000 |
| anomalia | False |

**Table 2: redes_moviles record fields**

| redes_moviles | |
|---|---|
| **Field** | **Example** |
| version | 1.0 |
| timestamp | 2021-02-25T11:00:32.000+0000 |
| id | de539085-315f-466a-81c1-55b97f5348df |
| type | RM |

| | |
|---|---|
| event | DATA |
| rat | 4G |
| imei | NA |
| imsi | 901700000013633 |
| time | 2021-01-27T09:52:01.000+0000 |
| anomalia | True |

**Table 3: trafico_ids record fields**

| **trafico_ids** | |
|---|---|
| **Field** | **Example** |
| prediction | 1 |
| scrip | 175.45.176.1 |
| sport | 0 |
| dstip | 149.171.126.12 |
| dsport | 80 |
| proto | tcp |
| version | 1.0 |
| id | f0c48ba4-387d-11ea-a137-2e728ce88126 |
| type | CS |
| event | DATA |
| time_stamp | 1602163578587 |

**Table 4: siem record fields**

| siem | |
|---|---|
| Field | Example |
| version | 1.0 |
| timestamp | 2021-02-25T10:32:12.000+0000 |
| id | f0c48ba4-387d-11ea-a137-2e728ce8812 |
| type | SM |
| event | DATA |
| Signature | AlienVault HIDS: Login session closed. |
| Date | 2021-02-22T13:39:00.000+0000 |
| Sensor | alienvault |
| Source | 0.0.0.0 |
| Destination | 0.0.0.0 |
| Risk | 0 |
| anomalia | False |

**Table 5: bluetooth record fields**

| **bluetooth** | |
|---|---|
| **Field** | **Example** |
| version | 1.0 |
| timestamp | 2021-02-25T10:02:24.000+0000 |
| id | f0c48ba4-387d-11ea-a137-2e728ce88126 |

| | |
|---|---|
| type | BT |
| event | DATA |
| status | offline |
| classic_mode | f |
| uuid | 0559ef63-e4c3-4d0c-a735-7105f29bfad2 |
| company | Texas Instruments Inc. (13) |
| updated_at | 2021-02-04T10:22:25.000+0000 |
| last_seen | 2021-02-04T10:22:25.000+0000 |
| uap_lap | 93:AB:5C:E1 |
| address | 18:7A:93:AB:5C:E1 |
| lmp_version | unknow |
| le_mode | t |
| manufacturer | unknow |
| created_at | 2021-02-04T10:22:25.000+0000 |
| name | Smart Watch |
| anomalia | True |

**Table 6: wifi record fields**

| **wifi** | |
|---|---|
| **Field** | **Example** |
| version | 1 |
| timestamp | 2021-02-25T11:32:13.000+0000 |
| id | f0c48ba4-387d-11ea-a137-2e728ce88126 |

| | |
|---|---|
| type | WF |
| event | DATA |
| userid | F0:03:8C:DF:33:23 |
| minact | 1 |
| tseen | 30 |
| tacum | 27240 |
| visits | 48 |
| act24h | 96 |
| pwr | -89 |
| footprint | 2E:1E:F7:32:08:9E |
| oui | azure |
| type_mac | MAL |
| tx_packets | 1 |
| tx_bytes | 84 |
| rx_packets | 0 |
| rx_bytes | 0 |
| ap | unknown |
| essid | unknown |
| apwr | -1 |
| time | 2021-02-02T11:45:00.000+0000 |
| anomalia | False |

**Table 7: firewall record fields**

| Firewall | |
|---|---|
| **Field** | **Example** |
| version | 1+F73:F73:F153 |
| timestamp | 2021-02-25T12:25:15.000+0000 |
| id | 5b83a05e-a69f-e3fc-5ece-93d600010005 |
| type | Connection |
| event | DATA |
| Time | 2020-05-27T11:22:46.000+0000 |
| Blade | Firewall |
| Action | Accept |
| Type | Connection |
| Interface | N/A |
| Origin | SMS-GW-CHECK |
| Source | SRV_DC_01 (10.1.200.11) |
| Source User Name | N/A |
| Destination | srv2.telconet.net (200.93.192.161) |
| Service | 'domain-udp (UDP/53) |
| Access Rule Number | 57 |
| Access Rule Name | Consulta DNS Domain Controllers |
| Policy Name | Standard |

| | |
|---|---|
| Description | domain-udp Traffic Accepted from 'srv-dc-01@coopcrea.fin.ec'(10.1.200.11) to 200.93.192.161 |
| Id | 5b83a05e-a69f-e3fc-5ece-93d600010005 |
| Marker | @A@@B@1590555605@C@2969330 |
| Log Server Login | SMS-GW-CHECK (10.1.201.1) |
| Interface Direction | inbound |
| Interface Name | eth1 |
| Connection Direction | Outgoing |
| Id Generated By Indexer | false |
| First | True |
| Sequencenum | 50 |
| Source Zone | Internal |
| Destination Zone | External |
| Service ID | domain-udp |
| Source Port | 64159 |
| Destination Port | 53 |
| IP Protocol | UDP (17) |
| Xlate (NAT) Source IP | SMS-GW-CHECK (179.49.29.10) |
| Xlate (NAT) Source Port | 54880 |

| | |
|---|---|
| Xlate (NAT) Destination Port | 0 |
| NAT Rule Number | 0 |
| NAT Additional Rule Number | 0 |
| Source Machine Name | srv-dc-01@coopcrea.fin.ec |
| Hll Key | 9435118931605540000 |
| Context Num | 1 |
| Policy Management | SMS-GW-CHECK |
| Db Tag | {10B41B45-4E19-A745-9231-AE1687566AA9} |
| Policy Date | Today 9:50:39 |
| Product Family | Access |
| Logid | 0 |
| Policy Rule UID | 629deb9c-68ad-410e-87fa-e14059f0bd88 |
| Layer Name | Network |
| Needs Browse Time | N/A |
| User | N/A |
| Src User Dn | N/A |
| Protocol | N/A |
| Sig Id | N/A |
| Reason | N/A |

| | |
|---|---|
| Destination Machine Name | N/A |
| Destination User Name | N/A |
| Dst User Dn | N/A |
| UserCheck ID | N/A |
| Destination Object | N/A |
| ICMP | N/A |
| ICMP Type | N/A |
| ICMP Code | N/A |
| Client Name | N/A |
| Product Version | N/A |
| Domain Name | N/A |
| Endpoint IP | N/A |
| Authentication Status | N/A |
| Identity Source | N/A |
| Session ID | N/A |
| Source Machine Group | N/A |
| Authentication Method | N/A |
| Identity Type | N/A |
| Authentication Trial | N/A |

| | |
|---|---|
| Source User Group | N/A |
| Connection Id | N/A |
| Last Update Time71 | N/A |
| Scheme | N/A |
| Methods | N/A |
| VPN Peer Gateway | N/A |
| Community | N/A |
| Mobile Access Session UID | N/A |
| VPN Feature | N/A |
| Duration | N/A |
| Last Update Time79 | N/A |
| Update Count | N/A |
| Creation Time | N/A |
| Connections | N/A |
| Aggregated Log Count | N/A |
| _c84 | N/A |
| anomalia | False |

**Table 8: ids_suricata ("fileinfo") record fields**

| ids_suricata (event_type=fileinfo) | | | |
|---|---|---|---|
| **Field** | **Example** | | |
| version | 1.0 | | |
| time | 1602677977.8111 | | |
| id | 2ee0bfe2-9aea-43f7-b481-7cc436407ead | | |
| type | IDS | | |
| event | DATA | | |
| data | timestamp | 2016-08-16T22:41:57.718668+0200 | |
| | flow_id | 1067121040688650 | |
| | pcap_cnt | 134 | |
| | event_type | fileinfo | |
| | src_ip | 186.33.233.170 | |
| | src_port | 80 | |
| | dest_ip | 192.168.4.202 | |
| | dest_port | 55392 | |
| | proto | TCP | |
| | http | hostname | www.nacionalmendoza.com.ar |
| | | url | / |
| | | http_user_agent | Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko |

| | | | |
|---|---|---|---|
| | | http_method | GET |
| | | protocol | HTTP/1.1 |
| | | status | 200 |
| | | length | 109012 |
| | app_proto | http | |
| | fileinfo | filename | / |
| | | sid | [] |
| | | gaps | False |
| | | state | TRUNCATED |
| | | stored | False |
| | | size | 103733 |
| | | tx_id | 0 |
| prediction | 1 | | |

**Table 9: ids_suricata ("flow") record fields**

| **Ids_suricata (event_type=flow)** | | | |
|---|---|---|---|
| **Field** | **Example** | | |
| version | 1.0 | | |
| time | 1602677977.81110 | | |
| id | 2ee0bfe2-9aea-43f7-b481-7cc436407ead | | |
| type | IDS | | |

| event | DATA | | |
|---|---|---|---|
| data | timestamp | 2016-08-16T22:41:57.718668+0200 | |
| | flow_id | 1067121040688650 | |
| | event_type | flow | |
| | src_ip | 186.33.233.170 | |
| | src_port | 80 | |
| | dest_ip | 192.168.4.202 | |
| | dest_port | 55392 | |
| | proto | TCP | |
| | app_proto | failed | |
| | flow | pkts_toserver | 5 |
| | | pkts_toclient | 4 |
| | | bytes_toserver | 352 |
| | | bytes_toclient | 280 |
| | | start | 2016-08-16T22:42:14.617652+0200 |
| | | end | 2016-08-16T22:42:16.172435+0200 |
| | | length | 109012 |
| | | age | 2 |
| | | state | closed |
| | | reason | shutdown |
| | | alerted | False |

| | | | |
|---|---|---|---|
| | tcp | tcp_flags | 1b |
| | | tcp_flags_ts | 1b |
| | | tcp_flags_tc | 1b |
| | | syn | True |
| | | fin | True |
| | | psh | True |
| | | ack | True |
| | | state | closed |
| prediction | 1 | | |

**Table 10: ids_suricata ("http") record fields**

| **Ids_suricata (event_type=http)** | | | |
|---|---|---|---|
| **Field** | **Example** | | |
| version | 1.0 | | |
| time | 1602677977.81110 | | |
| id | 2ee0bfe2-9aea-43f7-b481-7cc436407ead | | |
| type | IDS | | |
| event | DATA | | |
| data | timestamp | 2016-08-16T22:41:57.718668+0200 | |
| | flow_id | 1067121040688650 | |
| | pcap_cnt | 147 | |
| | event_type | http | |

| | | | |
|---|---|---|---|
| | src_ip | 186.33.233.170 | |
| | src_port | 80 | |
| | dest_ip | 192.168.4.202 | |
| | dest_port | 55392 | |
| | proto | TCP | |
| | tx_id | 0 | |
| | http | hostname | vtqckhl.hopto.org |
| | | url | /wordpress/?ARX8 |
| | | http_user_agent | Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko |
| | | http_content_type | text/html |
| | | http_refer | http://www.nacionalmendoza.com.ar/ |
| | | http_method | GET |
| | | protocol | HTTP/1.1 |
| | | status | 200 |
| | | length | 109012 |
| prediction | 1 | | |

**Table 11: ids_suricata ("alert") record fields**

| Ids_suricata (event_type=alert) | | | |
|---|---|---|---|
| **Field** | **Example** | | |
| | | | |
| version | 1.0 | | |
| time | 1602677977.81140 | | |
| id | 7d4ef1f2-40ed-4403-9476-a06b2a02392d | | |
| type | IDS | | |
| event | DATA | | |
| data | timestamp | 2016-08-16T22:41:57.718668+0200 | |
| | flow_id | 1067121040688650 | |
| | pcap_cnt | 134 | |

| | | | | |
|---|---|---|---|---|
| | event_type | alert | | |
| | src_ip | 192.168.4.202 | | |
| | src_port | 55416 | | |
| | dest_ip | 192.168.4.202 | | |
| | dest_port | 55392 | | |
| | proto | TCP | | |
| | tx_id | 1 | | |
| | alert | action | allowed | |
| | | gid | 1 | |
| | | signature_id | 2014726 | |
| | | rev | 126 | |
| | | signature | ET POLICY Outdated Flash Version M1 | |
| | | category | Potential Corporate Privacy Violation | |
| | | severity | 1 | |

| | | | | |
|---|---|---|---|---|
| | | metadata | updated_at | 2020_06_12 |
| | | | signature_severity | Informational |
| | | | performance_impact | Low |
| | | | former_category | POLICY |
| | | | created_at | 2012_05_09 |
| | | | affected_product | Adobe_flash |
| | http | hostname | cixiidae.recipmedia.co.uk | |
| | | url | /train/william-30066971.swf | |
| | | http_user_agent | Mozilla/5.0 (Windows NT 6.1; WOW64; Trident/7.0; rv:11.0) like Gecko | |
| | | http_content_type | application/x-shockwave-flash | |
| | | http_refer | http://cixiidae.recipmedia.co.uk/rifle/1993618/kindle-stiff-right | |
| | | http_method | GET | |

| | | | | |
|---|---|---|---|---|
| | | protocol | HTTP/1.1 | |
| | | status | 200 | |
| | | length | 109012 | |
| | app_proto | http | | |
| | flow | pkts_toserver | 7 | |
| | | pkts_toclient | 8 | |
| | | bytes_toserver | 1114 | |
| | | bytes_toclient | 5590 | |
| | | start | 2016-08-16T22:42:00.258387+0200 | |
| prediction | 1 | | | |

**Table 12: ids_suricata ("stats") record fields**

| **ids_suricata(event_type=stats)** | |
|---|---|
| **Field** | **Example** |

| | | | | | | |
|---|---|---|---|---|---|---|
| version | 1.0 | | | | | |
| time | 1602677977.81140 | | | | | |
| id | 7d4ef1f2-40ed-4403-9476-a06b2a02392d | | | | | |
| type | IDS | | | | | |
| event | DATA | | | | | |
| data | timestamp | 2016-08-16T22:41:57.718668+0200 | | | | |
| | event_type | stats | | | | |
| | stats | uptime | 45 | | | |
| | | decoder | pkts | 692 | | |
| | | | bytes | 55668 | | |
| | | | invalid | 0 | | |
| | | | ipv4 | 692 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | ipv6 | 0 | | |
| | | | ethernet | 692 | | |
| | | | raw | 0 | | |
| | | | null | 0 | | |
| | | | sll | 0 | | |
| | | | tcp | 692 | | |
| | | | udp | 0 | | |
| | | | sctp | 0 | | |
| | | | icmpv4 | 0 | | |
| | | | icmpv6 | 0 | | |
| | | | ppp | 0 | | |
| | | | pppoe | 0 | | |
| | | | gre | 0 | | |
| | | | vlan | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | vlan_qinq | 0 | | |
| | | | vxlan | 0 | | |
| | | | ieee8021ah | 0 | | |
| | | | teredo | 0 | | |
| | | | ipv4_in_ipv6 | 0 | | |
| | | | ipv6_in_ipv6 | 0 | | |
| | | | mpls | 0 | | |
| | | | avg_pkt_size | 789 | | |
| | | | max_pkt_size | 1372 | | |
| | | | erspan | 0 | | |
| | | | event | ipv4 | pkt_too_small | 0 |
| | | | | | hlen_too_small | 0 |
| | | | | | iplen_smaller_than_hlen | 0 |
| | | | | | trunc_pkt | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | opt_invalid | 0 |
| | | | | | opt_invalid_len | 0 |
| | | | | | opt_malformed | 0 |
| | | | | | opt_pad_required | 0 |
| | | | | | opt_eol_required | 0 |
| | | | | | opt_duplicate | 0 |
| | | | | | opt_unknown | 0 |
| | | | | | wrong_ip_version | 0 |
| | | | | | icmpv6 | 0 |
| | | | | | frag_pkt_too_large | 0 |
| | | | | | frag_overlap | 0 |
| | | | | | frag_ignored | 0 |
| | | | | icmpv4 | pkt_too_small | 0 |
| | | | | | unknown_type | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | unknown_code | 0 |
| | | | | | ipv4_trunc_pkt | 0 |
| | | | | | ipv4_unknown_ver | 0 |
| | | | | icmpv6 | unknown_type | 0 |
| | | | | | unknown_code | 0 |
| | | | | | pkt_too_small | 0 |
| | | | | | ipv6_unknown_version | 0 |
| | | | | | ipv6_trunc_pkt | 0 |
| | | | | | mld_message_with_invalid_hl | 0 |
| | | | | | unassigned_type | 0 |
| | | | | | experimentation_type | 0 |
| | | | | ipv6 | pkt_too_small | 0 |
| | | | | | trunc_pkt | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | trunc_exthdr | 0 |
| | | | | | exthdr_dupl_fh | 0 |
| | | | | | exthdr_useless_fh | 0 |
| | | | | | exthdr_dupl_rh | 0 |
| | | | | | exthdr_dupl_hh | 0 |
| | | | | | exthdr_dupl_dh | 0 |
| | | | | | exthdr_dupl_ah | 0 |
| | | | | | exthdr_dupl_eh | 0 |
| | | | | | exthdr_invalid_optlen | 0 |
| | | | | | wrong_ip_version | 0 |
| | | | | | exthdr_ah_res_not_null | 0 |
| | | | | | hopopts_unknown_opt | 0 |
| | | | | | hopopts_only_padding | 0 |
| | | | | | dstopts_unknown_opt | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | dstopts_only_padding | 0 |
| | | | | | rh_type_0 | 0 |
| | | | | | zero_len_padn | 0 |
| | | | | | fh_non_zero_reserved_field | 0 |
| | | | | | data_after_none_header | 0 |
| | | | | | unknown_next_header | 0 |
| | | | | | icmpv4 | 0 |
| | | | | | frag_pkt_too_large | 0 |
| | | | | | frag_overlap | 0 |
| | | | | | frag_ignored | 0 |
| | | | | | ipv4_in_ipv6_wrong_version | 0 |
| | | | | | ipv6_in_ipv6_too_small | 0 |
| | | | | | ipv6_in_ipv6_wrong_version | 0 |
| | | | | tcp | pkt_too_small | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | hlen_too_small | 0 |
| | | | | | invalid_optlen | 0 |
| | | | | | opt_invalid_len | 0 |
| | | | | | opt_duplicate | 0 |
| | | | | udp | pkt_too_small | 0 |
| | | | | | hlen_too_small | 0 |
| | | | | | hlen_invalid | 0 |
| | | | | sll | pkt_too_small | 0 |
| | | | | ethernet | pkt_too_small | 0 |
| | | | | ppp | pkt_too_small | 0 |
| | | | | | vju_pkt_too_small | 0 |
| | | | | | ip4_pkt_too_small | 0 |
| | | | | | ip6_pkt_too_small | 0 |
| | | | | | wrong_type | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | unsup_proto | 0 |
| | | | | pppoe | pkt_too_small | 0 |
| | | | | | wrong_code | 0 |
| | | | | | malformed_tags | 0 |
| | | | | gre | pkt_too_small | 0 |
| | | | | | wrong_version | 0 |
| | | | | | version0_recur | 0 |
| | | | | | version0_flags | 0 |
| | | | | | version0_hdr_too_big | 0 |
| | | | | | version0_malformed_sre_hdr | 0 |
| | | | | | version1_chksum | 0 |
| | | | | | version1_route | 0 |
| | | | | | version1_ssr | 0 |
| | | | | | version1_recur | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | version1_flags | 0 |
| | | | | | version1_no_key | 0 |
| | | | | | version1_wrong_protocol | 0 |
| | | | | | version1_malformed_sre_hdr | 0 |
| | | | | | version1_hdr_too_big | 0 |
| | | | | vlan | header_too_small | 0 |
| | | | | | unknown_type | 0 |
| | | | | | too_many_layers | 0 |
| | | | | ieee8021ah | header_too_small | 0 |
| | | | | ipraw | invalid_ip_version | 0 |
| | | | | ltnull | pkt_too_small | 0 |
| | | | | | unsupported_type | 0 |
| | | | | sctp | pkt_too_small | 0 |
| | | | | | wrong_code | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | | malformed_tags | 0 |
| | | | | mpls | header_too_small | 0 |
| | | | | | pkt_too_small | 0 |
| | | | | | bad_label_router_alert | 0 |
| | | | | | bad_label_implicit_null | 0 |
| | | | | | bad_label_reserved | 0 |
| | | | | | unknown_payload_type | 0 |
| | | | | erspan | header_too_small | 0 |
| | | | | | unsupported_version | 0 |
| | | | | | too_many_vlan_layers | 0 |
| | | | dce | pkt_too_small | 0 | |
| | | flow | memcap | 0 | | |
| | | | tcp | 9 | | |
| | | | udp | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | icmpv4 | 0 | | |
| | | | icmpv6 | 0 | | |
| | | | spare | 9996 | | |
| | | | emerg_mode_entered | 0 | | |
| | | | emerg_mode_over | 0 | | |
| | | | tcp_reuse | 0 | | |
| | | | memuse | 7475616 | | |
| | | defrag | ipv4 | fragments | 0 | |
| | | | | reassembled | 0 | |
| | | | | timeouts | 0 | |
| | | | ipv6 | fragments | 0 | |
| | | | | reassembled | 0 | |
| | | | | timeouts | 0 | |
| | | | max_frag_hits | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | flow_bypassed | local_pkts | 0 | | |
| | | | local_bytes | 0 | | |
| | | | local_capture_pkts | 0 | | |
| | | | local_capture_bytes | 0 | | |
| | | | closed | 0 | | |
| | | | pkts | 0 | | |
| | | | bytes | 0 | | |
| | | tcp | sessions | 9 | | |
| | | | ssn_memcap_drop | 0 | | |
| | | | pseudo | 0 | | |
| | | | pseudo_failed | 0 | | |
| | | | invalid_checksum | 0 | | |
| | | | no_flow | 0 | | |
| | | | syn | 9 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | synack | 9 | | |
| | | | rst | 1 | | |
| | | | midstream_pickups | 0 | | |
| | | | pkt_on_wrong_thread | 0 | | |
| | | | segment_memcap_drop | 0 | | |
| | | | stream_depth_reached | 0 | | |
| | | | reassembly_gap | 0 | | |
| | | | overlap | 1 | | |
| | | | overlap_diff_data | 0 | | |
| | | | insert_data_normal_fail | 0 | | |
| | | | insert_data_overlap_fail | 0 | | |
| | | | insert_list_fail | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | memuse | 573440 | | |
| | | | reassembly_memuse | 98304 | | |
| | | detect | engines | id | 0 | |
| | | | | last_reload | 2020-10-14T14:19:30.029249+0200 | |
| | | | | rules_loaded | 21053 | |
| | | | | rules_failed | 0 | |
| | | | alert | 3 | | |
| | | app_layer | flow | http | 4 | |
| | | | | ftp | 0 | |
| | | | | smtp | 0 | |
| | | | | tls | 0 | |
| | | | | ssh | 0 | |
| | | | | imap | 0 | |

| | | | | | |
|---|---|---|---|---|---|
| | | | | smb | 0 |
| | | | | dcerpc_tcp | 0 |
| | | | | dns_tcp | 0 |
| | | | | nfs_tcp | 0 |
| | | | | ntp | 0 |
| | | | | ftp-data | 0 |
| | | | | tftp | 0 |
| | | | | ikev2 | 0 |
| | | | | krb5_tcp | 0 |
| | | | | dhcp | 0 |
| | | | | snmp | 0 |
| | | | | failed_tcp | 3 |
| | | | | dcerpc_udp | 0 |
| | | | | dns_udp | 0 |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | nfs_udp | 0 | |
| | | | | krb5_udp | 0 | |
| | | | | failed_udp | 0 | |
| | | | tx | http | 0 | |
| | | | | ftp | 0 | |
| | | | | smtp | 0 | |
| | | | | tls | 0 | |
| | | | | ssh | 0 | |
| | | | | imap | 0 | |
| | | | | smb | 0 | |
| | | | | dcerpc_tcp | 0 | |
| | | | | dns_tcp | 0 | |
| | | | | nfs_tcp | 0 | |
| | | | | ntp | 0 | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | | ftp-data | 0 | |
| | | | | tftp | 0 | |
| | | | | ikev2 | 0 | |
| | | | | krb5_tcp | 0 | |
| | | | | dhcp | 0 | |
| | | | | snmp | 0 | |
| | | | | dcerpc_udp | 0 | |
| | | | | dns_udp | 0 | |
| | | | | nfs_udp | 0 | |
| | | | | krb5_udp | 0 | |
| | | | expectations | 0 | | |
| | | flow_mgr | closed_pruned | 0 | | |
| | | | new_pruned | 0 | | |
| | | | est_pruned | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | bypassed_pruned | 0 | | |
| | | | flows_checked | 4 | | |
| | | | flows_notimeout | 4 | | |
| | | | flows_timeout | 0 | | |
| | | | flows_timeout_inuse | 0 | | |
| | | | flows_removed | 0 | | |
| | | | rows_checked | 65536 | | |
| | | | rows_skipped | 0 | | |
| | | | rows_empty | 65532 | | |
| | | | rows_busy | 0 | | |
| | | | rows_maxlen | 1 | | |
| | | http | memuse | 0 | | |
| | | | memcap | 0 | | |
| | | ftp | memuse | 0 | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | | | memcap | 0 | | |
| predictio n | 1 | | | | | |