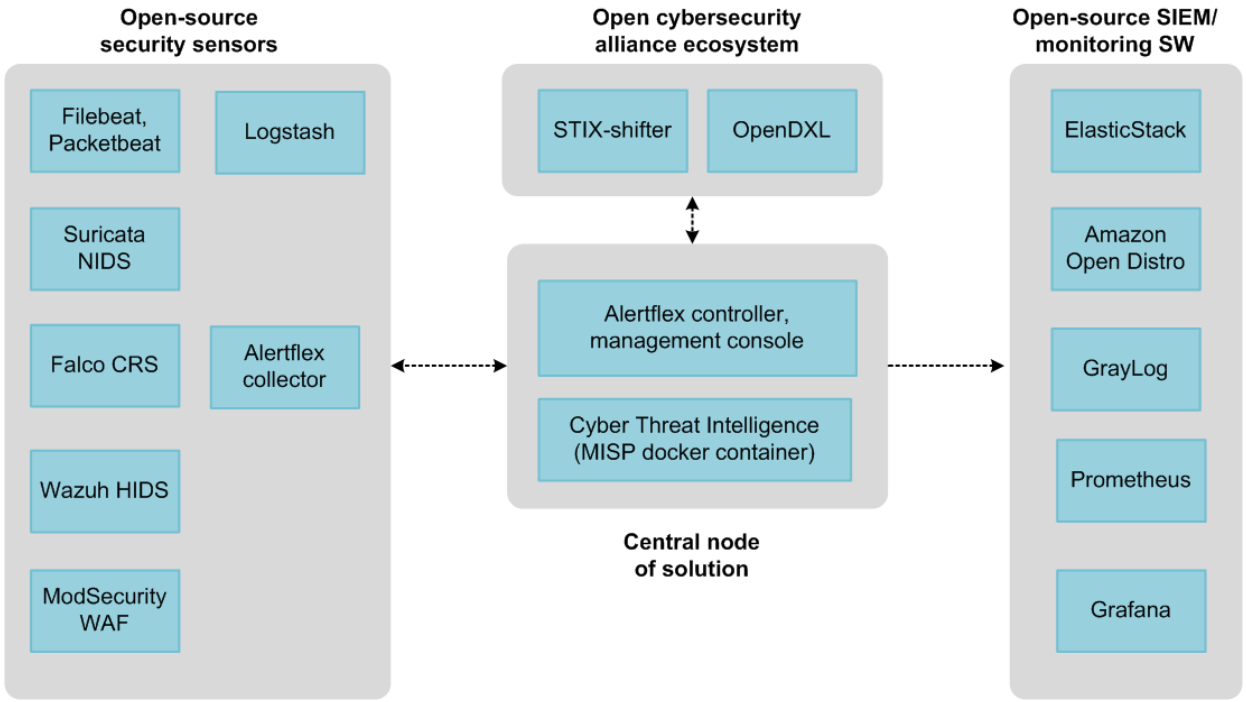
Alertflex open source version



Advantages of Alertflex

Alertflex distributed architecture is optimally suited for use in Hybrid Clouds (public/private clouds, on-premises). Alertflex data model supports multi-tenancy and micro-segmentation.

The solution includes own security event management system, deeply integrated with sources of security events - Wazuh HIDS, Suricata NIDS, Modsecurity WAF and Falco Container IDS.

For security events exchanges, Alertflex uses ActiveMQ which is PCI and SOC compliance. ActiveMQ is an official message broker for Amazon AWS services and RedHat OpenShift platform.

Alertflex collector (Altprobe)

Altprobe was designed special for manage of security sensors and provide two-way communication:

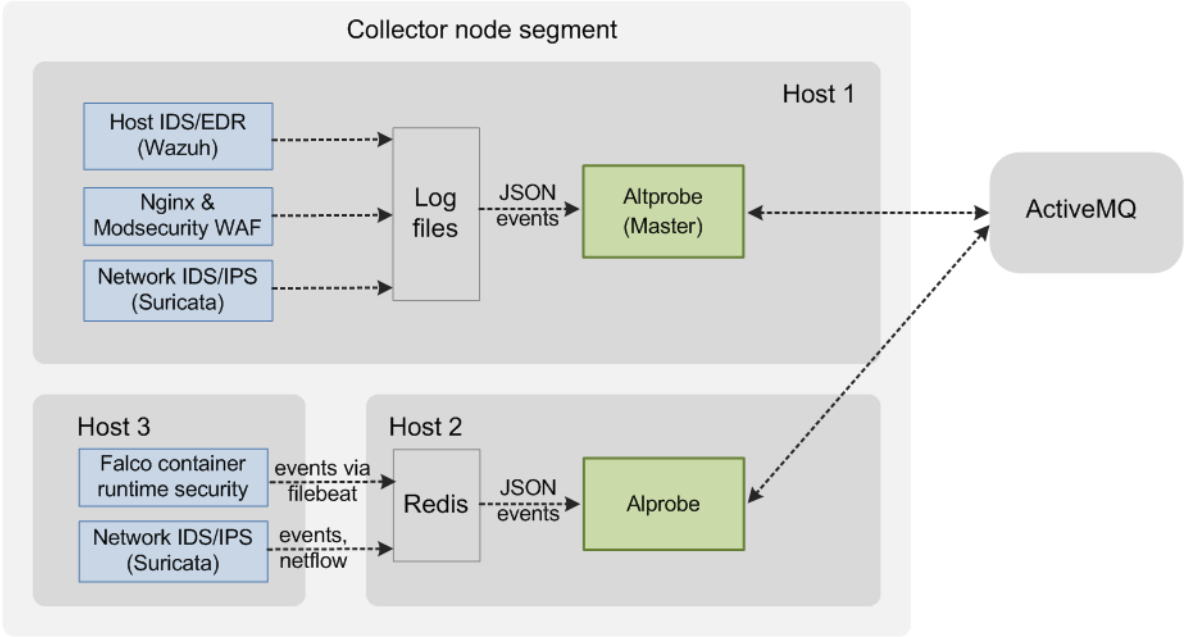
From IDS sensor to Altprobe

- Security events
- Backup of IDS rules and configs
- Inventory events

From Altprobe to IDS sensors

- Update IDS rules and configs
- Active response for Wazuh
- Create agents for Wazuh

Altprobe performs normalization, aggregation and apply filtering policy for IDS security events

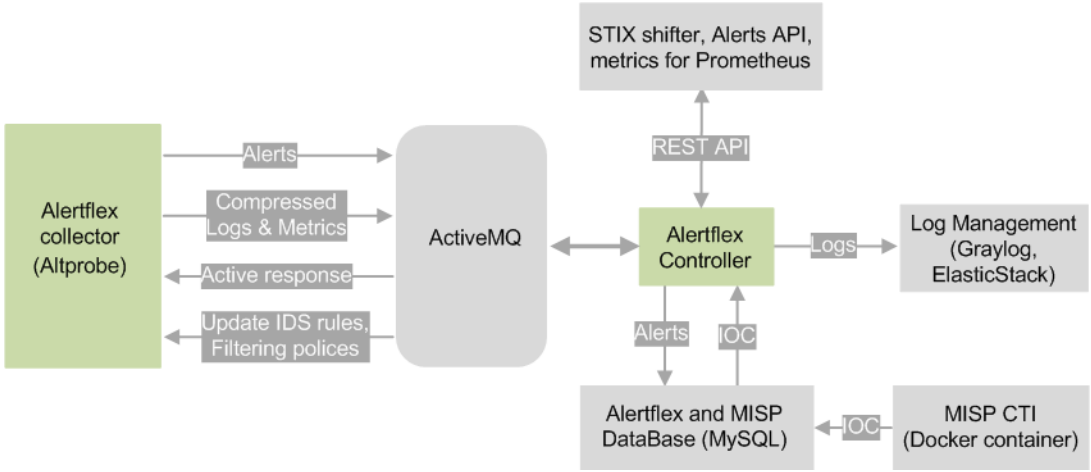


Example filtering policy:

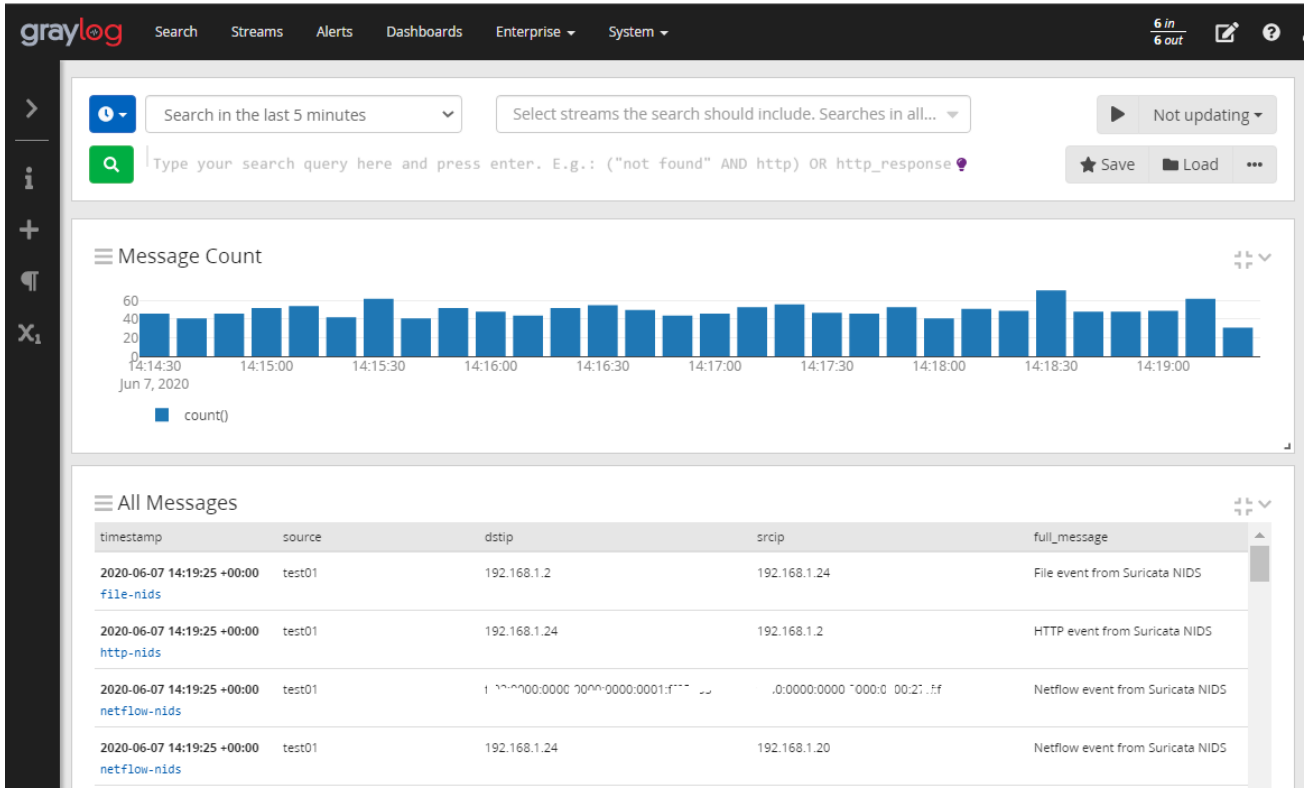
```
"hids": {
        "gray_list": [{
                "event": "5715",
                "agent": "flghost",
                "match": "indef",
                "aggregate": {
                        "reproduced": 0,
                        "in_period": 0
                },
                "response": {
                        "profile": "indef",
                        "new_type": "indef",
                        "new_source": "indef",
                        "new_event": "55715",
                        "new_severity": 1,
                        "new_category": "new cat",
                        "new_description": "new desc"
                }
        ]}
}
```

Alertflex controller

• Saves IDS alerts in Alertflex database (MySQL)
• Can redirect alerts to Graylog, ElasticStack, OpenDistro log management platforms
• Provides a REST API for alerts, STIX shifter, metrics for Prometheus
• Performs a reputation checks for IP addresses, DNS records, MD5, SHA1 and SHA256 hashes of files. Creates an alert, in case of suspicious data has been found.
• Performs analysis of different reports (OpenSCAP, Wazuh SCA, etc). Creates an alert if a new vulnerability, misconfigurations, processes or packages has been found.



Example Suricata Netflow events transmitted from Alertflex to Graylog



Example Prometheus/Grafana dashboard for Alertflex collector metrics

Example STIX shifter request for Wazuh FIM alerts:

[alert:type = 'FILE']


```
"objects": {
            "0": {
              "type": "file",
              "hashes": {
                "SHA-1": "d7ec10f7a229c13b49257e3d9227b73537f40090",
                "MD5": "423999f949bbd9116df704876620d5ab"
              }
            },
            "1": {
              "type": "file",
              "name": "/etc/alertflex/test01/master-hids/remrules/0030-postfix_rules.xml"
            }
          },
          "x_org_alertflex": {
            "severity": 2,
            "agent": "flghost",
            "description": "Integrity checksum changed.",
            "source": "Wazuh",
            "type": "FILE",
            "node": "test01",
            "event": "550",
            "category": "ossec, syscheck, pci_dss_11.5, hipaa_164.312.c.1, hipaa_164.312.c.2, gdpr_II_5.1.f, nist_800_53_SI.7",
```

Example STIX shifter request for Suricata IDS alerts:

[alert:severity = 3 AND alert:source = 'Suricata']


```
"0": {
                "type": "ipv4-addr",
                "value": "192.168.1.2"
            },
            "1": {
                "type": "network-traffic",
                "src_ref": "0",
                "dst_port": 9000,
                "protocols": [
                    "ip"
                ],
                "src_port": 41872,
                "dst_ref": "2"
            },
            "2": {
                "type": "ipv4-addr",
                "value": "192.168.1.24"
            }
        },
        "x_org_alertflex": {
            "severity": 3,
            "description": "ET POLICY Outgoing Basic Auth Base64 HTTP Password detected unencrypted"
```