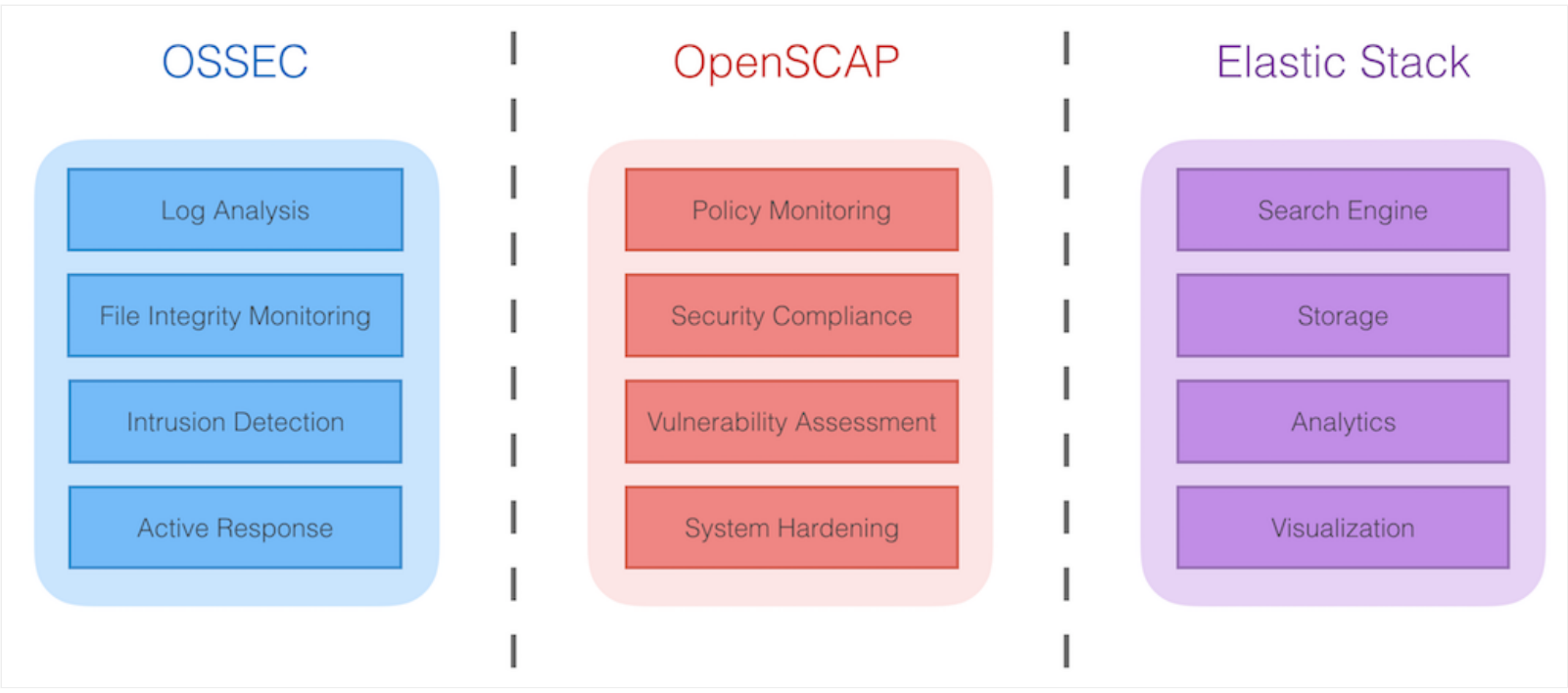
Getting started

Wazuh is a security detection, visibility, and compliance open source project. It was born as a fork of OSSEC HIDS, later was integrated with Elastic Stack and OpenSCAP evolving into a more comprehensive solution. Below is a brief description of these tools and what they do:



OSSEC HIDS

OSSEC HIDS is a Host-based Intrusion Detection System (HIDS) used both for security detection, visibility, and compliance monitoring. It's based on a multi-platform agent that forwards system data (e.g log messages, file hashes, and detected anomalies) to a central manager, where it is further analyzed and processed, resulting in security alerts. Agents convey event data to the central manager via a secure and authenticated channel.

Additionally, OSSEC HIDS provide a centralized syslog server and an agentless configuration monitoring system, providing security insight into the events and changes on agentless devices such as firewalls, switches, routers, access points, network appliances, etc.

OpenSCAP

OpenSCAP is an OVAL (Open Vulnerability Assessment Language) and XCCDF (Extensible Configuration Checklist Description Format) interpreter used to check system configurations and to detect vulnerable applications.

It's a well-known tool designed to check the security compliance and hardening of the systems using industry standard security baselines for enterprise environments.

Elastic Stack

Elastic Stack is a software suite (Filebeat, Logstash, Elasticsearch, Kibana) used to collect, parse, index, store, search, and present log data. It provides a web frontend useful for gaining a high-level dashboard view of events, as well to realize advanced analytics and data mining deep into your store of event data.

Table of Contents

This document will help you understand Wazuh components and its architecture, Also, it will show you some common use cases.

- Security policy monitoring