Wazuh - An Open Source SIEM/XDR Solution

November 07, 2023

By Aaron Grothe

Introduction

If anybody has any questions or comments at any time please let me know.

If I start to mumble please let me know as well :-)

Wazuh???

Wazuh is an Open Source XDR, SIEM Solution.

I promise you I'm not making up those terms.

SIEM???

What is a SIEM?

Security Information and Event Management

Combines

Security Information Management (inventory, assets, installed soft, etc.)
Security Event Management (brute force login attempt, etc)

XDR?

eXtended Detection and Response

What is XDR?

Security incident detection and response

E.g. if a system detects a brute force login attack it might automatically add a firewall rule to block the attack

Is Wazuh Really Open Source?

- Yep
  - GPL version 2
  - Apache 2.0 License
  - Migrated from Elasticsearch (BSL) to OpenSearch (APL 2.0)
- Wazuh used OSSEC as a base and has added OpenSearch, Kibana to it to make it more scalable user friendly

How does Wazuh make money?

- Services
  - Professional Services
  - Consulting Services
  - Cloud Hosting of Wazuh Servers
  - Reseller Partnerships

What makes up Wazuh?

Wazuh by default consists of the following components

Wazuh Host/Server - tend to use Host/Server interchangeably

- Wazuh indexer - Opensearch based search engine
- Wazuh Server - Analyzes data processes through rules
- Wazuh Dashboard - Kibana based front end

Wazuh Agent - Simple Agent

- Supports Linux, Windows, Mac OS X, Solaris, AIX, HPux

What if my system isn't supported?

Wazuh supports RSyslog if your system doesn't work a Wazuh agent

You'll be doing this if you want to do docker or kubernetes logging

Given this the system is able to support almost everything in your enterprise. If not write a module for it.

Monitoring - AWS Instances

To give you an idea of what Wazuh can monitor in AWS or for most regular systems, we'll talk about the following

- log data collection
- file integrity monitoring
- malware detection
- security policy monitoring
- system inventory
- vulnerability detection

Monitoring - AWS Services

Wazuh can also monitor various AWS Services

- S3
- WAF
- VPC
- Cloudwatch Logs
- Amazon Security Lake

Not sure if you'd wanting all of these logs or you'd monitor them through Amazon services, but still nice to have

Monitoring - Other Cloud Providers

Wazuh can also monitor other cloud providers/services

- Microsoft Azure - Instances, Activity, and Services
- GCP services - Cloud Storage, Pub/Sub
- Microsoft Office 365 - Activity
- Microsoft Graph - Activity

Monitoring - Github

Github monitoring is kind of cool. It covers most of what you'd want to see monitored

- audit log
- access to your organization or repository settings
- changes in permission
- added or removed users in an org, repository, or team
- users promoted to admin
- changes to permission of a github app
- git events: cloning, fetching and pushing

If you're monitoring all cloning, you might see a lot of events

Regulatory Compliance

Wazuh Has guides for the following

- PCI DSS Compliance
- GPDR Compliance
- HIPAA COmpliance
- NIST 800-53 Compliance
- TSC Compliance

The PCI DSS documentation is pretty good

Demo

We've talked a lot about what Wazuh can do:

We'll do a Demo

This demo is very simple

Debian 12 - Host
Debian 12 - Agent
Ubuntu 20.04 Agent

Gives a decent overview of the systems

How do you customize it

Reviewing the file for the configuration

/var/ossec/etc/ossec.conf

There are actually two versions of this file on a system.

The version hosted on the server, values set in this one override the values in the clients

Time to Talk about some of the Options

We'll go over options for the following

- Virtualization Options
- Trusted VM Options
- Secure Network Options

There are a lot of options here, so let's get started

Five Things I Wish I Had Know at First

1. Do not go under the recommendations for the host system - 8gb ram, 4 cores, and plenty of disk space
2. Make the host a recommended OS: Red Hat Enterprise Linux 7, 8, 9; CentOS 7, 8; Amazon Linux 2; Ubuntu 16.04, 18.04, 20.04, 22.04
3. It is going to be noisy. Keep in mind until you tune/tame it
4. Gradual rollout, while there is an ansible playbook for it, don't roll it out wide until you got it pared down
5. Be very careful about allowing the system to do an remmediation, you want to have quite a bit of experience before you let it make changes

Is Wazuh Worth Trying?

YES!!!

If you have a need for a SIEM solution Wazuh is well worth investigating further.

If you need PCI, HIPPA or any of the other supported regulatory compliance Wazuh can save you a lot of time

If the Server will support RPI 5s, I might buy an 8gb version of that and set it up to at least do syslog forwarding from my systems, and probably put the agent on some of my more critical systems

Links

Wazuh - https://wazuh.com

Network Chuck's introduction to Wazuh - https://www.youtube.com/watch?v=3CaG2GI1kn0

John Hammond on Wazuh https://www.youtube.com/watch?v=3CaG2GI1kn0

Thanks and Q&A

That's all I've got for tonight.

Thanks for Listening.

Any Questions???