Suricata en wazuh

***Waarom suricata?***

* ***is IDS maar kan ook draaien als IPS (d.m.v packet capturing)***
* ***kan ook netwerkmonitoring***
* ***werkt goed samen met het SIEM(wazuh)***

***Waarom wazuh?***

* ***Ingebouwde siem-tool***
* ***Goeie intergratie met suricata***
* ***Wazuh kan gemakkelijk integreren met Suricata, een IDS/IPS-systeem, om netwerkbedreigingen te detecteren. De logs van Suricata worden verzameld en gecorreleerd door Wazuh, wat zorgt voor een gedetailleerd overzicht van zowel netwerk- als hostgebeurtenissen.***

Afbeelding met tekst, Lettertype, schermopname, wit

Automatisch gegenereerde beschrijving  
Logging doormiddel van SIEM tooling, waarbij file transfers en system logins worden meegerekend

In het SIEM dienen wijzigingen in bestanden op fileshares gelogd te worden, net als alle toegang naar het internet van alle medewerkers en studenten via de proxies

|  |  |
| --- | --- |
| IDS |  |
| Suricata | IDS of IPS om netwerkverkeer te monitoren en verdachte activiteiten te detecteren. |
| Wazuh Agent | Stuurt logbestanden en beveiligingsgegevens naar de Wazuh Manager op de SIEM-server. |
| Filebeat | Verzamelt logbestanden van Suricata en verzendt deze naar Elasticsearch (via de SIEM-server). |

|  |  |
| --- | --- |
| SIEM |  |
| Wazuh Manager | Verzamelt gegevens van Wazuh Agent en integreert deze met Elasticsearch en Kibana. |
| Elasticsearch | Slaat loggegevens op en indexeert deze voor snelle zoekopdrachten. |
| Kibana | Geeft een visuele interface voor het analyseren en monitoren van loggegevens. |

***Conclusie***

**Wazuh** biedt SIEM-functionaliteiten door systeemlogs te analyseren.

**Suricata** detecteert netwerkgebaseerde aanvallen. (IDS/IPS)

**Filebeat** zorgt voor logverzameling en verzending naar Elasticsearch.

**Elasticsearch** slaat logs op en maakt het mogelijk om deze te doorzoeken.

**Kibana** visualiseert de gegevens en maakt analyses mogelijk.

Wat nu overblijft, is de configuratie van alle onderdelen. Zodra Suricata logs genereert, deze via Filebeat naar Elasticsearch stuurt, en Kibana de data visualiseert, heb je een volledig werkend IDS.

**Wat doet dit playbook?**

**sudo ansible-playbook -i inventory.ini install\_suricata.yml**

**Wazuh Installatie:**

* Bijwerken van de apt-cache en installatie van de vereiste pakketten.
* Toevoegen van de Wazuh GPG-sleutel en repository.
* Installeren van de Wazuh Manager en het starten van de service.

**Suricata Installatie:**

* Toevoegen van de Suricata repository en installatie van Suricata.
* Starten en inschakelen van de Suricata service.

**Elasticsearch Installatie:**

* Toevoegen van de Elasticsearch GPG-sleutel en repository.
* Installeren van Elasticsearch, aanpassen van de configuratie voor een enkele node.
* Starten en inschakelen van Elasticsearch.

**Kibana Installatie:**

* Installeren van Kibana en configureren om toegankelijk te zijn vanaf alle interfaces.
* Starten en inschakelen van Kibana.

**Integratie van Wazuh met Elasticsearch:**

* Aanmaken van de map voor de Wazuh Elasticsearch template.
* Downloaden en toevoegen van de Wazuh template aan Elasticsearch.
* Starten van Filebeat en configureren voor Wazuh logs.

inclusief Filebeat voor logverwerking

***Bestandwijzigingen op fileshares monitoren met Wazuh's FIM.***  
Wazuh File Integrity Monitoring (FIM): Wazuh kan wijzigingen in bestanden en mappen detecteren en loggen door middel van zijn ingebouwde (FIM). Je kunt specifieke fileshares of directories configureren om wijzigingen, creaties, of verwijderingen bij te houden.

***Internettoegang via proxies monitoren met Suricata.***  
Suricata kan netwerkverkeer inspecteren en loggen, inclusief HTTP-, HTTPS-, DNS- en andere soorten verkeer die via de proxy gaan.

***Systeemlogins monitoren met Wazuh (auditd en log analysis).***

**Wazuh Auditd en Log Analysis:** Wazuh kan authenticatiepogingen (geslaagd en mislukt) loggen door middel van:

* **Log analysis:** Analyseert systeemlogboeken (zoals /var/log/auth.log in Linux of Event Logs in Windows).
* **Auditd integration:** Detecteert specifieke gebeurtenissen zoals logins, sudo-gebruik, en privilege-escalaties.