**Suricata** i **Snort** su dva popularna alata za mrežnu sigurnost koja služe za detekciju i prevenciju napada na mreži. Oba su sustava za analizu prometa i zaštitu od intruzija, ali imaju određene razlike u funkcionalnostima i performansama.

**1. Snort**

Snort je jedan od najpoznatijih i najduže postojećih sistema za detekciju i prevenciju upada .On analizira mrežni promet u stvarnom vremenu, traži sumnjive aktivnosti i upozorava administratore na potencijalne napade.

**Čemu služi Snort?**

* **IDS (Intrusion Detection System):** Snort analizira mrežni promet u stvarnom vremenu i traži uzorke koji odgovaraju poznatim napadima, kao što su napadi DoS (Denial of Service), skeniranje portova, pokušaji iskorištavanja sigurnosnih rupa itd.
* **IPS (Intrusion Prevention System):** Uz detekciju, Snort može poduzeti akcije u realnom vremenu, poput blokiranja sumnjivih paketa ili IP adresa.
* **Zabilježavanje i analiza logova:** Snort stvara logove koji mogu biti korisni za post-mortem analize napada ili mrežnih aktivnosti.

**Kako se koristi Snort?**

* Snort se najčešće koristi na Linux/Unix sustavima, ali može raditi i na Windowsu.
* Snort se pokreće u načinu nadzora (IDS) ili prevencije (IPS) i mora biti konfiguriran s pravilima koja će detektirati specifične napade.
* Korisnici mogu koristiti Snort-ov CLI (command-line interface) za postavljanje i upravljanje pravilima, dok se za vizualizaciju podataka može koristiti neki od integriranih alata, poput **Barnyard2** (za obrada logova) ili **Snorby** (za vizualizaciju podataka).

**2. Suricata**

Suricata je noviji alat koji je također IDS/IPS sustav, ali nudi dodatne značajke u odnosu na Snort, poput boljih performansi i podrške za multithreading, što ga čini bržim i skalabilnijim.

**Čemu služi Suricata?**

* Kao i Snort, Suricata služi za detekciju i prevenciju napada, analizirajući mrežni promet i tražeći specifične obrasce (potpuno analitički pristup).
* **Protokoli i usluge:** Suricata je također bolja u analizi složenijih protokola poput HTTP, DNS, SMTP i drugih, kao i u otkrivanju napada temeljenih na aplikacijama.
* **Veća brzina:** Podržava multithreading
* **Logiranje i analiza:** Suricata može generirati bogate logove koji omogućuju detaljnu analizu napada ili sumnjivih aktivnosti.

**Kako se koristi Suricata?**

* Suricata se koristi na istim platformama kao i snort
* Kao i Snort, koristi pravila koja omogućuju prepoznavanje sumnjivih obrazaca, ali nudi i dodatne značajke kao što su detekcija napada na temelju TLS/SSL certifikata, DDoS napadi itd.
* Za rad s Suricatom, potrebno je instalirati pravila (na primjer, **Emerging Threats** ili **Suricata-Update** za automatsko ažuriranje pravila).
* Suricata može raditi u "IDS" ili "IPS" modu, ovisno o potrebama sustava.
* Također, Suricata je dobro integrirana s alatima za analizu kao što su **Elasticsearch**, **Kibana** i **Logstash** (tzv. ELK stack).

**Razlike između Snorta i Suricate**

* **Performanse:** Suricata je dizajnirana za bolje performanse, osobito u visokim protokolema (high throughput). To je zbog bolje podrške za multithreading podataka, što je čini skalabilnijom.
* **Protokoli i analiza:** Suricata ima napredniju analizu aplikacijskih protokola i bolje razumijevaje protokola kao što su DNS, HTTP, i SSL/TLS.
* **Kompatibilnost sa Snort pravilima:** Suricata može koristiti Snort pravila, ali nudi i dodatne vlastite značajke.

**Zaključak:**

* **Snort** je stariji i stabilan sustav, vrlo popularan u sigurnosnoj zajednici, dok **Suricata** nudi bolje performanse, napredniju analizu i širu podršku za modernije tehnologije.
* Besplatni, open-source
* Snort je možda bolji za manja okruženja ili specifične use-caseove, dok je Suricata često bolji za veće mreže i zahtjevnije analize.