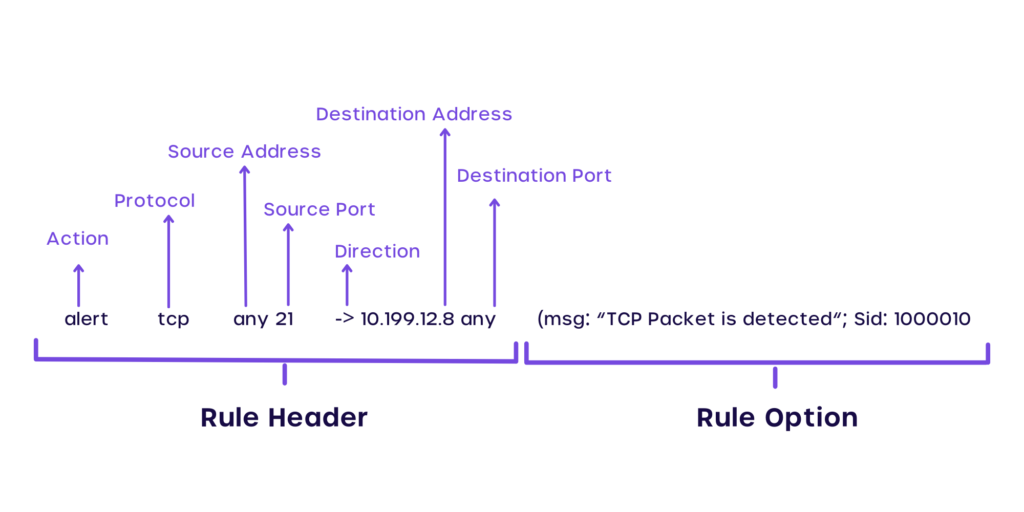
Snort هي أداة مفتوحة المصدر تستخدم في (Intrusion detection) و (Intrusion prevention) و تحتوي على مجموعة من القواعد التي تحدد التصرف المطلوب فعله, تقدم خيار ممتاز للمؤسسات لإمكانية التعديل و التخصيص بما يتناسب مع احتياجات المنظمة.

تتكون قواعد Snort من التالي:

* التصرف عند المطابقة
* البروتكول
* عنوان IP المرسل
* منفذ المرسل
* الاتجاه
* عنوان IP المستقبل
* منفذ المستقبل
* رسالة تحذيرية
* معرف خاص بالقاعدة

***صوره للتوضيح فقط***



مصادر:

<https://cyvatar.ai/write-configure-snort-rules/>

https://www.snort.org/