Reçoit les paquets depuis une interface en mode promiscuous	Capture un paquet Ethernet complet
Voit passer une trame ARP	Ecoute le trafic HTTP sur le port 80
Enregistre un paquet ICMP (ping)	Capture tout le trafic réseau sans filtre
Bloque une connexion	Sépare les couches réseaux (Ethernet, IP, TCP, HTTP, ...)
Lit l'IP source et destination	Note le port utilisé (80, 443, 22, ...)
Décode l'en-tête IP (TTL, checksum, fragmentation)	Interprète la requête HTTP (GET /index.html)

Reconnaît le protocole de transport (UDP ou TCP)

Voit que le paquet est chiffré en TLS

Reconstruit un flux TCP à partir de plusieurs paquets

Compare le contenu du flux HTTP avec une signature SNORT

Recherche une règle "si SELECT * FROM alors alerte SQL injection"

Compte le nombre de SYN sans ACK pour détecter un scan SYN flood

Repère une tentative de shellcode dans le payload

Analyse une règle "alerte si plus de 100 connexions en 1 minute"

Exécute une règle de détection de malware dans un fichier téléchargé

Détecte une requête ICMP Echo envoyée à une adresse de broadcast avec une IP source falsifiée

Vérifie si l'IP source est sur une liste noire

Ecrit une alerte dans son fichier de logs

Envoie une alerte à la console d'administration

Transmet l'alerte vers un SIEM

Envoie un email au responsible sécurité

Déclenche une notification SNMP

Bloque immédiatement le paquet

Supprime le malware