Marcelo Henrique de Souza – 5° seg noturno

SURICATA

Foi apresentado a solução Suricata, que é um mecanismo de detecção de ameaças.
Possui código aberto
Possui bastante robustez como bloquear sites maliciosos, ips, hosts
Baseados por um conjunto de regras definidos pelo usuário
Inspeciona o tráfego de rede utilizando regras poderosas e banco de dados de assinaturas.
Utliza os modelos detecção de intrusão em tempo real, prevenção de intrusão em linha, monitoramento de segurança em rede e monitoramento de backup offline.
Possui os modos IDS e IPS
Possui técnicas de detecção baseados em assinatura, anomalias e análise de protocolos.
Ferramenta de Fácil instalação

Para intalar o Suricata dentro do Pfsenses vá em System>Package Manager> avaiable packages e pesquise por Suricata
para fazer a configuração vá em Services>Suricata
Em Global Settings podemos configurar para utilizar as assinaturas do Snort.