WAF nedir?

Waf son kullanıcı ile istek yapılan web sunucusu arasında bulunan, web sitesine veya web uygulamasına gidip gelen veri paketlerini izleyen, filtreleyen ve engelleyen bir güvenlik duvarıdır . Waf OSI'nin 7. katmanı olan uygulama katmanında görev alır ve adından da anlaşılabileceği gibi web uygulamalarını olası saldırılara karşı korumayı hedefler. Son kullanıcı ile sunucu arasında oluşan iletişimi dinleyerek tanımlanan kurallara göre filtreleme, düzeltme veya engelleme uygular.

Firewall Nedir?

Bilgisayar sistemleri için üretilen güvenlik duvarı sistemleridir. Firewall cihazları ise bu yazılımların uygun donanımlarla birleştirilerek üretilmesinden meydana gelmiş olan fiziksel ürünlerdir.

Bu bilgiler doğrultusunda Bilgi Güvenliği Müdürlüğü tarafından kullanılan Splunk ürünü arama örnekleri yapılmıştır. Aramalarda temel amaç üründe kullanılan waf ve firewall takılmış olan IP adresleri, personel sicilleri, atak konumları, atak tipi gibi bilgilerin elde edilmesidir. Bu sayede log analizi yapılıp, gerekli önlemler alınabilecektir.

Kod:

```
{
  index=f5 (action=”blocked” OR action=”alerted”)
  | stats count(eval(action=”alerted”)) as AlertedCount
  | stats count(eval(action=”blocked”)) as BlockedCount by src_ip,policy_name
  | sort – BlockedCount
  | iplocation src_ip
  | stats list(AlertedCount),list(BlockedCount) limit=5 by policy_name
  | head 10
}
```