Web Application Firewall
(Negative Security)
Mart 2024

Yasal Sorumluluk

Bu raporun hazırlanması ve bulgulara erişilmesi esnasında, her ne kadar azami dikkat gösterilse de rapordaki olası hatalardan ‘ZenithDefense’ sorumlu tutulamaz.

Bu raporda var olan önerilerin uygulanması sonucunda oluşabilecek problemlerden ‘ZenithDefense’ direk veya dolaylı olarak sorumlu tutulamaz.

Raporda çıkan sonuçlara ulaşmak için yapılan testler ve erişilen veriler raporu okuyanlar tarafında da test edilip gözlenmelidir.

Yorumlar ve sonuçlar hakkında veriler “ZenithDefense”’e ait olup izinsiz kopyalanıp kullanılamaz, bir kanıt olarak kullanılamaz.

Bu raporu okuyanlar yukarıda yazılanları kabul etmiş sayılır.

İçindekiler

1. Waf Hakkında Genel Bilgiler

Web Uygulama Güvenlik Duvarı, bir web uygulamasının önündeki filtre gibidir ve web uygulamalarına karşı gerçekleştirilen potansiyel tehditleri engellemek, tespit etmek ve önlemek amacıyla kullanılır. Bu güvenlik önlemi, uygulama katmanında (HTTP trafiği üzerinde) çalışarak çeşitli saldırılara karşı koruma sağlar. SQL enjeksiyonu, cross-site scripting (XSS), cross-site request forgery (CSRF) gibi yaygın saldırıları önleyerek web uygulamalarını daha güvenli hale getirir.

Web Uygulama Güvenlik Duvarı'nın (WAF) temelinde iki farklı güvenlik yaklaşımı bulunur: negatif güvenlik (negative security) ve pozitif güvenlik (positive security). Bu iki yaklaşım arasındaki temel farklar:

Negatif Güvenlik (Negative Security):

- İzin Verilenlerin Dışındakilere Odaklanır: Negatif güvenlik yaklaşımı, bilinen saldırı imzalarını algılayıp engellemeye odaklanır. Yani tanımlı kötü niyetli trafik işaretlerini tespit ederek bu trafikleri engeller.
- İmza Tabanlıdır: Negatif güvenlik, saldırıları tanımlamak için önceden tanımlanmış imzaları kullanır. Bu imzalar bilinen saldırıları temsil eder ve WAF bu imzaları tespit edip saldırıları engeller.
- Düşük Yanlış(False) Pozitif Oranı: Negatif güvenlik, genellikle düşük yanlış pozitif oranına sahiptir çünkü sadece bilinen kötü niyetli trafikleri engeller. Ancak yeni veya önce görülmemiş saldırıları tespit etme yeteneği sınırlı olabilir.

Pozitif Güvenlik (Positive Security):

- İzin Verilenleri Tanımlar: Pozitif güvenlik yaklaşımı, yalnızca belirli güvenilir trafik desenlerini ve davranışlarını tanımlamaya odaklanır. Yani sadece belirlenmiş olan doğru trafiği kabul eder ve diğerlerini engeller.
- Yapı Tabanlıdır: Pozitif güvenlik, güvenli trafik desenlerini tanımlamak için belirli bir yapı veya model kullanır. Bu model uygulama trafik desenlerini öğrenerek normal davranışı belirler ve bu davranış dışındaki istekleri engeller.
- Yüksek Yanlış Pozitif Oranı: Pozitif güvenlik, genellikle yüksek yanlış pozitif oranına sahiptir çünkü sadece tanımlı güvenli trafik desenlerini kabul eder ve bu desen dışındaki istekleri engeller. Bu yüzden yanlışlıkla güvenli trafikleri de engelleyebilir.

Hangi Yaklaşım Daha İyi?

Her iki yaklaşımın da kendine özgü avantajları ve dezavantajları vardır. Negatif güvenlik bilinen saldırıları etkili bir şekilde engelleyebilirken, pozitif güvenlik daha önce görülmemiş saldırıları tespit edebilir ve daha esnek bir koruma sağlayabilir. Hangi yaklaşımın tercih edileceği, uygulamanın gereksinimlerine ve risk profiline bağlıdır. Bazı durumlarda her iki yaklaşımın bir kombinasyonu da kullanılabilir.

Bir yapı düşünelim. Yaklaşık 200 adet uygulaması olsun. Bu 200 uygulamaya negatif security uygulamak çok da zor değildir, imza tabanlı olduğundan haftalık olarak kritik imzaları güncelleyip false positive ayıklamak gerekecektir.

Ancak bu 200 uygulama için positive security uygulamak çok zordur. Negative security %5 zamanımızı alırken düzgün bir positive security kalan %95 zamanımızı alır. Her uygulama için ayrı politika seti ayarlayıp, bunları uygulamak, muazzam bir işgücüdür. Ayrıca bu tarafta ürünlerin harcadığı kaynaklar çok fazla olduğundan, ölçeklendirme (sizing) olarak da yüksek maliyetlere neden olabilir.

Tüm bunların dışında uygulama önünde her ne kadar WAF cihazları koyulsa da, uygulamaya erişmek için bu path'in kullanılması zorunlu olmayabilir. Topolojiksel açıklıklar ve yanlış konfigürasyon kaynaklı, kötü niyetli kullanıcılar, WAF, IPS gibi ürünlere uğramadan uygulamanıza direk erişebilir. Bu kısım 'Network Security' makalemizde ayrıca değinilmiştir. Dileyenler o makalemize de bakabilir.

Bazı üreticilerin on-prem WAF ürünlerinde positive security bulunurken, aynı üreticinin Cloud ürününde positive security hiç bulunmayabilir.

Biz bu makalede Negative Security tarafında on-prem LTM ürünü üzerinde çalışan WAF, aynı üreticiden Linux üzerinde çalışan bir WAF bir de open source WAF ürünü üzerinde bir çalışma yaptık.

Yaptığımız çalışma bütün ürünler için benzer bir tablo ortaya çıkardı. Özet olarak negative security tarafında çok daha düşük maliyetler ile birbirine yakın korumaların sağlanabileceği sonucuna ulaştık. Sizler de kendi test metodoloji ve araçlarınız ile benzer testleri gerçekleştirip, buna göre bir karar verebilirsiniz.

2. Test edilen ürünler

a. F5-On Prem Waf

F5 WAF (Web Application Firewall), F5 Networks tarafından geliştirilen ve web uygulamalarını çeşitli siber tehditlere karşı korumak için kullanılan bir güvenlik çözümüdür. F5 WAF, web uygulamalarının önünde bulunan bir güvenlik duvarı gibi çalışır ve gelen HTTP/HTTPS trafiğini izler, analiz eder ve kötü niyetli aktivitelere karşı koruma sağlar. F5 WAF hakkında bilmeniz gereken bazı temel özellikler:

1. **Gelişmiş Saldırı Koruması:** F5 WAF, çeşitli siber saldırı türlerine karşı koruma sağlar. SQL enjeksiyonu, cross-site scripting (XSS), cross-site request forgery (CSRF), bot saldırıları ve daha fazlası gibi yaygın saldırıları algılar ve önler.
2. **Dinamik Öğrenme ve Özelleştirilebilir Kural Setleri:** F5 WAF, uygulama trafiğini dinamik olarak izleyerek normal trafik desenlerini öğrenir ve anormal aktiviteleri tespit eder. Ayrıca kuruluşların ihtiyaçlarına göre özelleştirilebilen kapsamlı kural setleri sunar.
3. **Uygulama DoS (Denial of Service) Koruması:** F5 WAF, uygulama hizmet reddi (DoS) saldırılarına karşı koruma sağlar. Anormal trafik desenlerini tespit eder ve bu tür saldırılara karşı önlemler alarak uygulamaların hizmet dışı kalmasını önler.
4. **SSL/TLS Trakik Şifreleme ve İşlem:** F5 WAF, HTTPS trafiğini deşifre etmek ve analiz etmek için SSL/TLS terminasyonu ve yeniden şifreleme yetenekleri sunar. Bu sayede şifreli trafik de koruma altına alabilir.
5. **Gelişmiş Analiz ve Raporlama:** F5 WAF, uygulama trafiğini ayrıntılı olarak izler ve analiz eder. Kullanıcı etkinliği, saldırılar, hatalar ve diğer olaylar hakkında kapsamlı raporlar sunar.
6. **Bulut ve Veri Merkezi Entegrasyonu:** F5 WAF, hem bulut ortamlarında (AWS, Azure, Google Cloud Platform) hem de veri merkezlerinde kullanılabilir. Bu kuruluşların çoklu ortamlarda güvenlik konsolidasyonu sağlamasına yardımcı olur.

F5 WAF, geniş kapsamlı güvenlik özellikleri sunan, ölçeklenebilir ve esnek bir çözümdür. Web uygulamalarının güvenliğini artırmak ve çeşitli saldırılara karşı koruma sağlamak isteyen kuruluşlar için önemli bir güvenlik yatırımı olarak değerlendirilebilir.

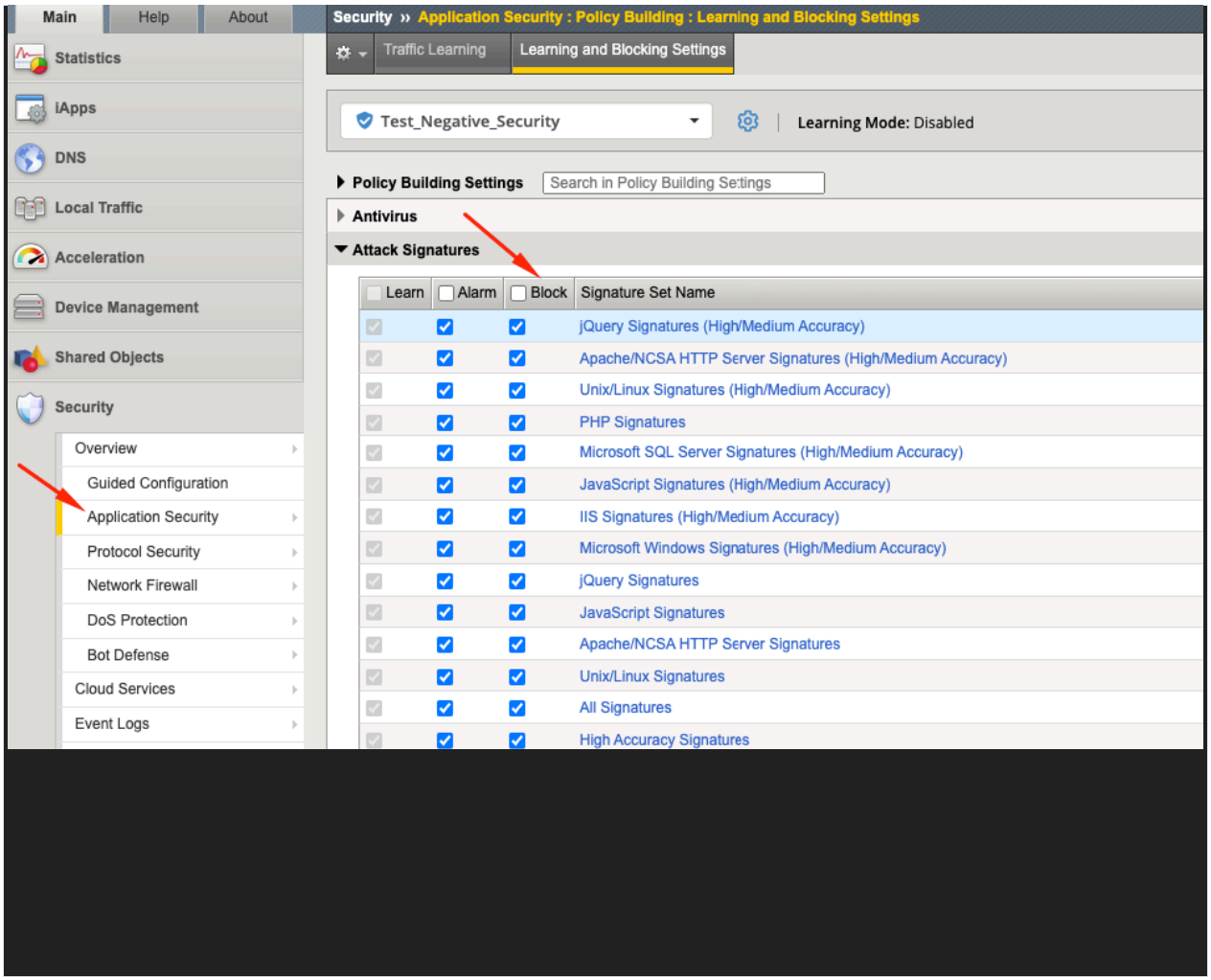
Bizim testlerimizde makalenin başında da belirtildiği üzere negative security üzerinden yol alınmıştır.

Dosya uzantısı olarak https://clouddocs.f5.com/bigip-next/latest/waf_management/awaf_policy_file_types.html adresindeki sadece;

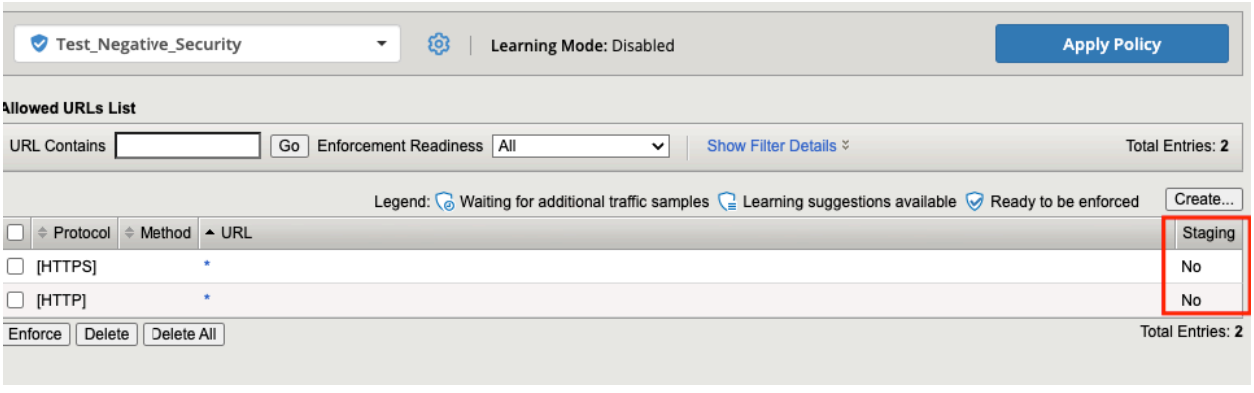
- Executable files: exe, msi, bin, cmd, com, bat, dll, sys

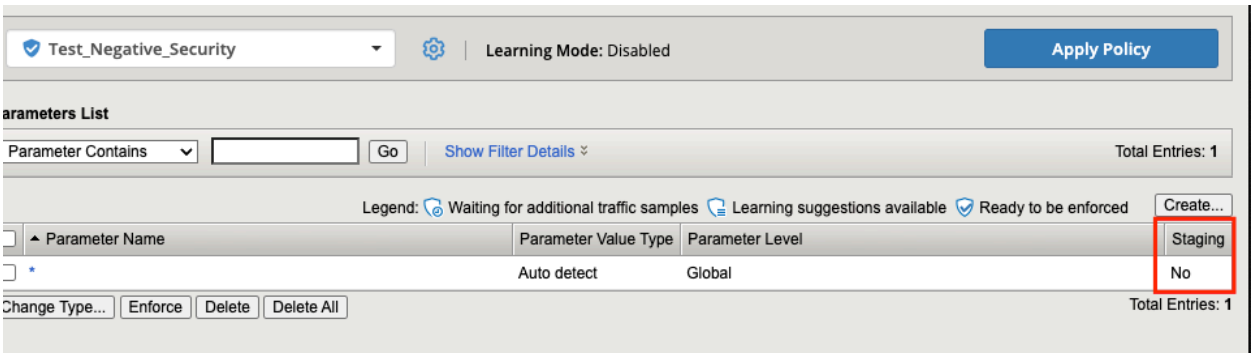
Dosya tipleri engellenmiştir.

Atak imza seti olarak sadece signature base imzalar açılmıştır.



Staging kısımları da enforce edilmişir.





Belirtiliği gibi standart konfigürasyonlar yapılarak, testler gerçekleştirilmiştir.

Test sonucu elde edilen koruma skoru 86 olmuştur. Test metodolojisi hakkında bilgi son bölümde (Ek1) verilmiştir.

b. F5-Nginx App Protect

Nginx Plus, temel açık kaynak kodlu Nginx web sunucu yazılımının bir ticari sürümüdür ve bir dizi ek özellik ve destek ile birlikte gelir. Nginx Plus, daha yüksek performans, gelişmiş ölçeklenebilirlik ve ileri düzey özellikler sunarak büyük ölçekli ve kritik uygulamalar için ideal bir çözüm sunar. Nginx Plus App Protect ise, Nginx Plus'ın bir parçası olarak gelen bir güvenlik modülüdür.

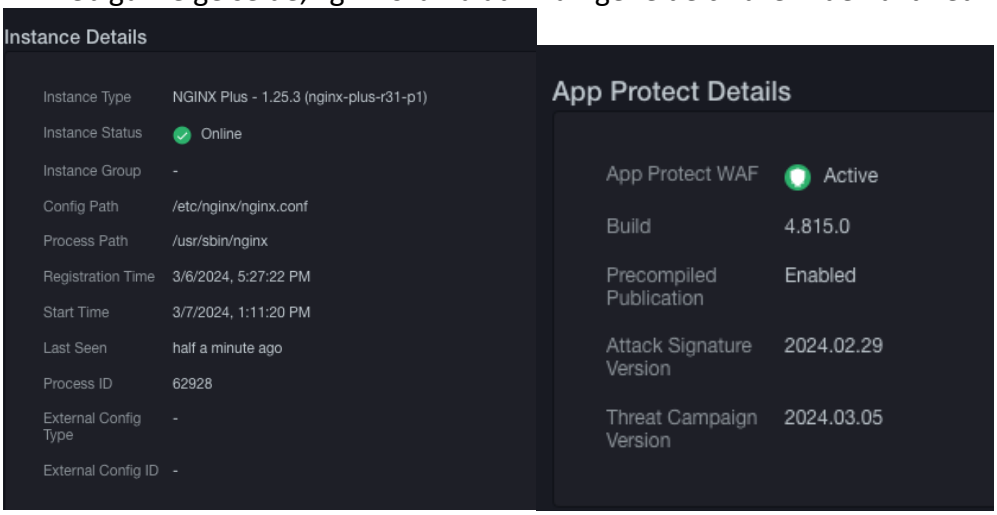
Nginx Plus App Protect Özellikleri:

1. **Web Uygulama Güvenlik Duvarı (WAF):** Nginx Plus App Protect, web uygulamalarını çeşitli siber tehditlere karşı korumak için bir WAF olarak kullanılabilir. Bu özellik, uygulama katmanındaki saldırılara karşı önlemler alır ve potansiyel tehditleri tespit ederek engeller.
2. **ModSecurity Entegrasyonu:** Nginx Plus App Protect, ModSecurity WAF motoruyla entegre çalışabilir. Bu, geniş bir saldırı imza veritabanına ve özelleştirilebilir kurallar setine erişim sağlayarak çeşitli saldırılara karşı koruma sağlar.
3. **Zengin Günlük ve İstatistikler:** App Protect, uygulama güvenliği olaylarını izlemek ve analiz etmek için kapsamlı günlük ve istatistikleri destekler. Bu sayede, güvenlik olaylarına hızlı bir şekilde müdahale edilebilir ve saldırıların detaylı analizi yapılabilir.
4. **API Koruma:** Nginx Plus App Protect, API'larınızı ve mikroservislerinizi korumak için özel olarak tasarlanmıştır. API trafiğini izleyebilir, koruyabilir ve güvenlik ihlallerine karşı önlemler alabilir.
5. **Kara Liste ve Beyaz Liste Desteği:** İstenmeyen trafikleri tanımlamak ve engellemek için IP adresi, ülke veya belirli kullanıcıları kara liste veya beyaz liste ekleyebilirsiniz.
6. **Hafif ve Yüksek Performanslı:** Nginx'in temel özellikleri olan hafif ve yüksek performanslı yapısı, App Protect ile birleşerek web uygulamalarınızın güvenliğini artırırken performans kaybını minimize eder.

Sonuç olarak;
Nginx Plus App Protect, Nginx Plus'ın güvenlik özellikleri arasında yer alan bir güvenlik modülüdür. Bu, web uygulamalarınızın ve API'larınızın güvenliğini sağlamak ve siber tehditlere karşı koruma önlemleri almak için güçlü bir çözüm sunar. Uygulama güvenliği önemli bir konu olduğundan, Nginx Plus App Protect gibi güvenlik önlemlerini etkin bir şekilde kullanmak, web uygulamalarınızın dayanıklılığını artırabilir ve siber saldırılara karşı güvende kalmanıza yardımcı olabilir.

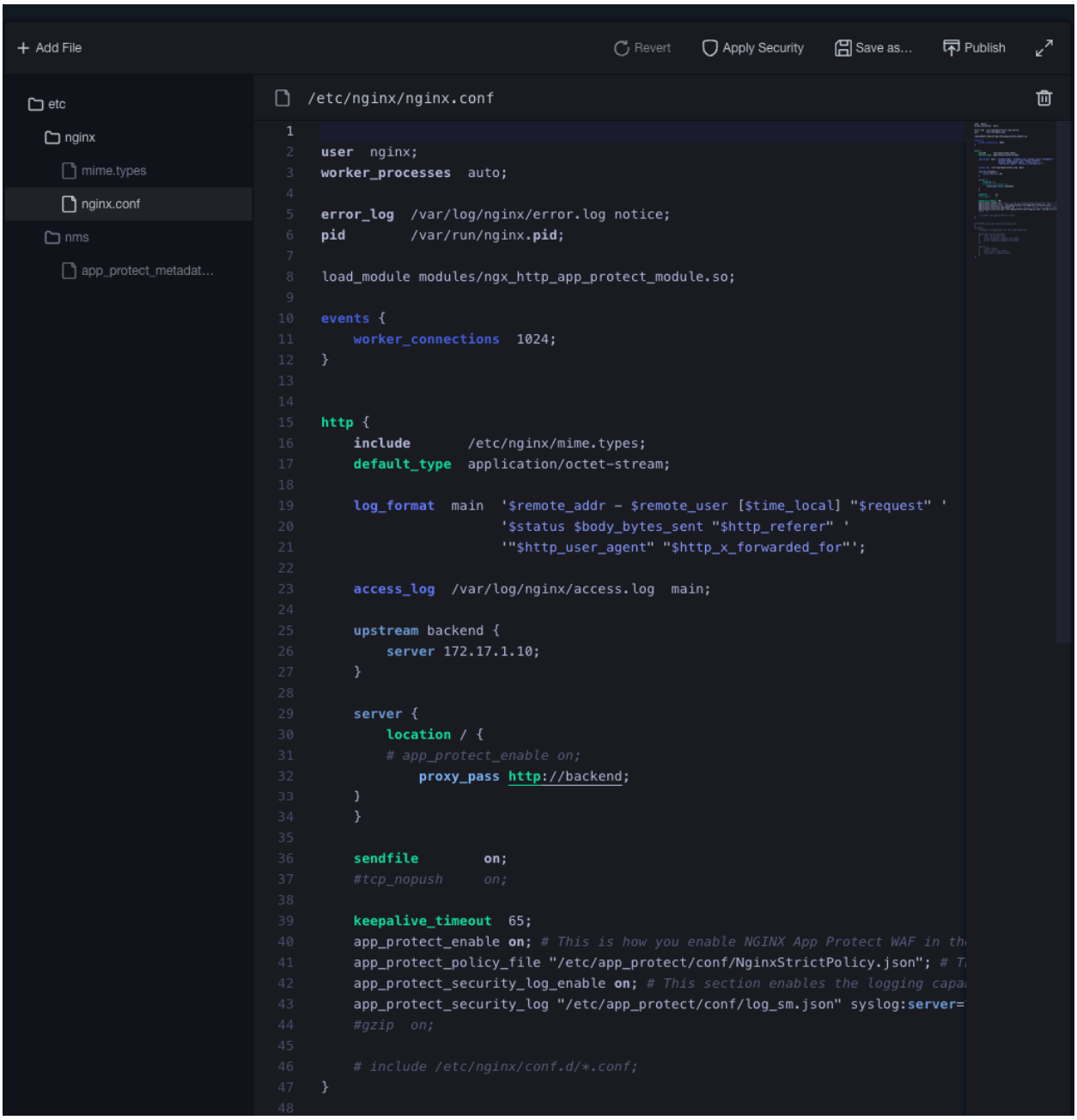
https://docs.nginx.com/nginx-app-protect-waf/ adresindeki yönergeleri takip ederek kolayca kurulumu sağlayabilirsiniz. Trial lisans olarak register olunarak hızlıca temin edilebiliyor.

Bir web gui ile gelse de, ilgili koruma adımları genelde cli üzerinden aktif ediliyor.

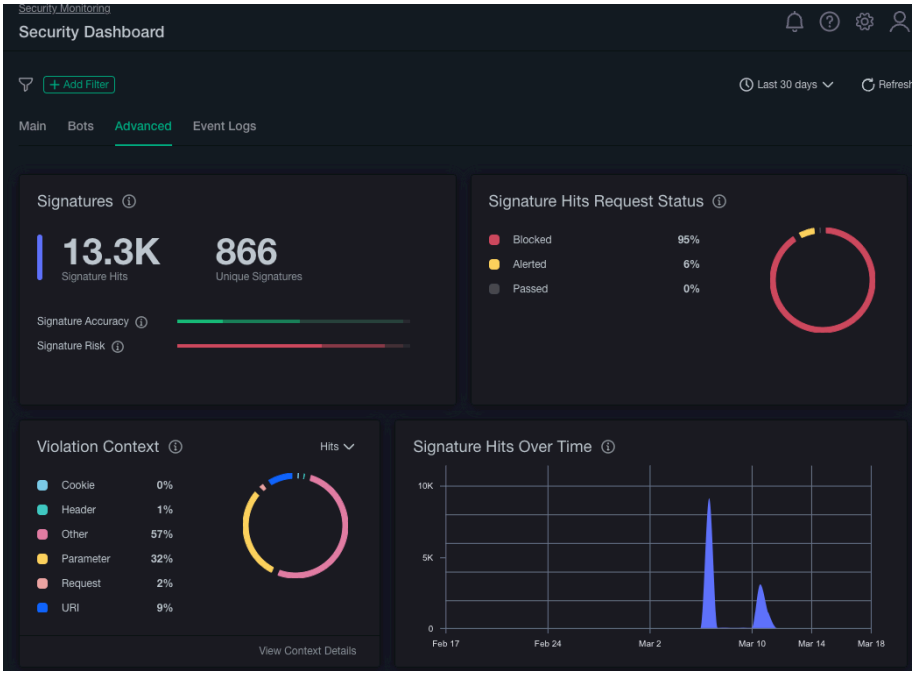


Aşağıda yer alan konfigürasyonda, LTM arkasına basit bir node alarak, xff'i aktif edip default olarak gelen "`NginxStrictPolicy.json`" politikasını kullandık.

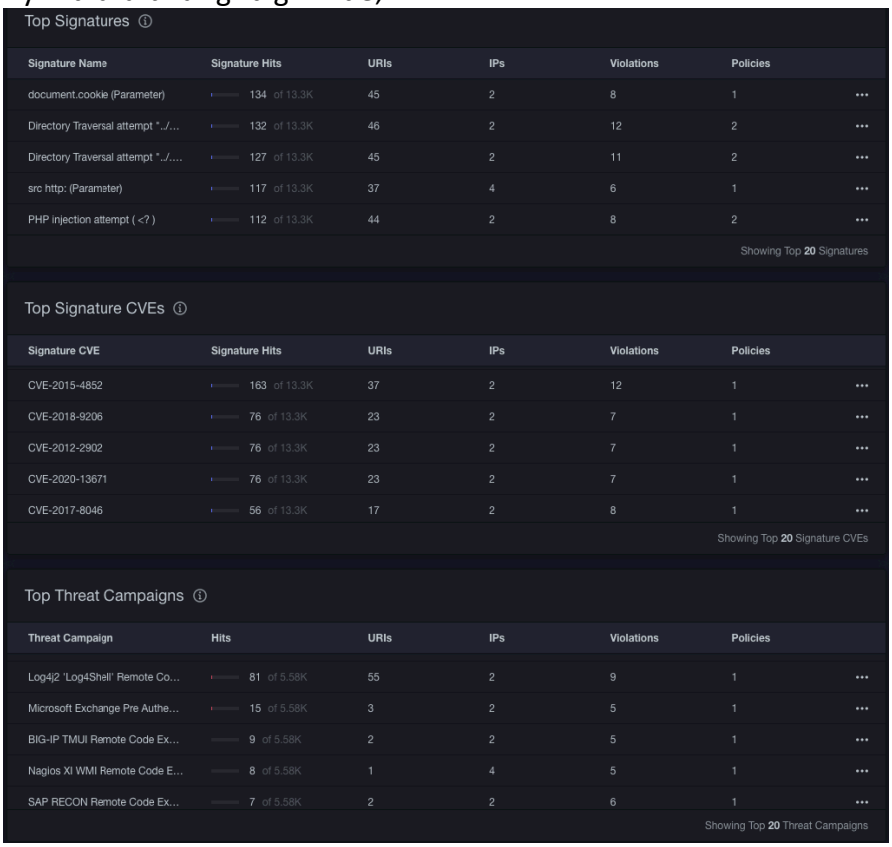
İlgili konfigürasyon bilgisi bir sonraki sayfada da yer almaktadır.


Add File
Revert
Apply Security
Save as...
Publish
etc
nginx
mime.types
nginx.conf
nms
app_protect_metadat...
/etc/nginx/nginx.conf
user nginx;
worker_processes auto;
error_log /var/log/nginx/error.log notice;
pid /var/run/nginx.pid;
load_module modules/ngx_http_app_protect_module.so;
events {
worker_connections 1024;
}
http {
include /etc/nginx/mime.types;
default_type application/octet-stream;
log_format main '$remote_addr - $remote_user [$time_local] "$request" '
'$status $body_bytes_sent "$http_referer" '
'"$http_user_agent" "$http_x_forwarded_for"';
access_log /var/log/nginx/access.log main;
upstream backend {
server 172.17.1.10;
}
server {
location / {
# app_protect_enable on;
proxy_pass http://backend;
}
}
sendfile on;
#tcp_nopush on;
keepalive_timeout 65;
app_protect_enable on; # This is how you enable NGINX App Protect WAF in th
app_protect_policy_file "/etc/app_protect/conf/NginxStrictPolicy.json"; # T
app_protect_security_log_enable on; # This section enables the logging capa
app_protect_security_log "/etc/app_protect/conf/log_sm.json" syslog:server=
#gzip on;
# include /etc/nginx/conf.d/*.conf;
}

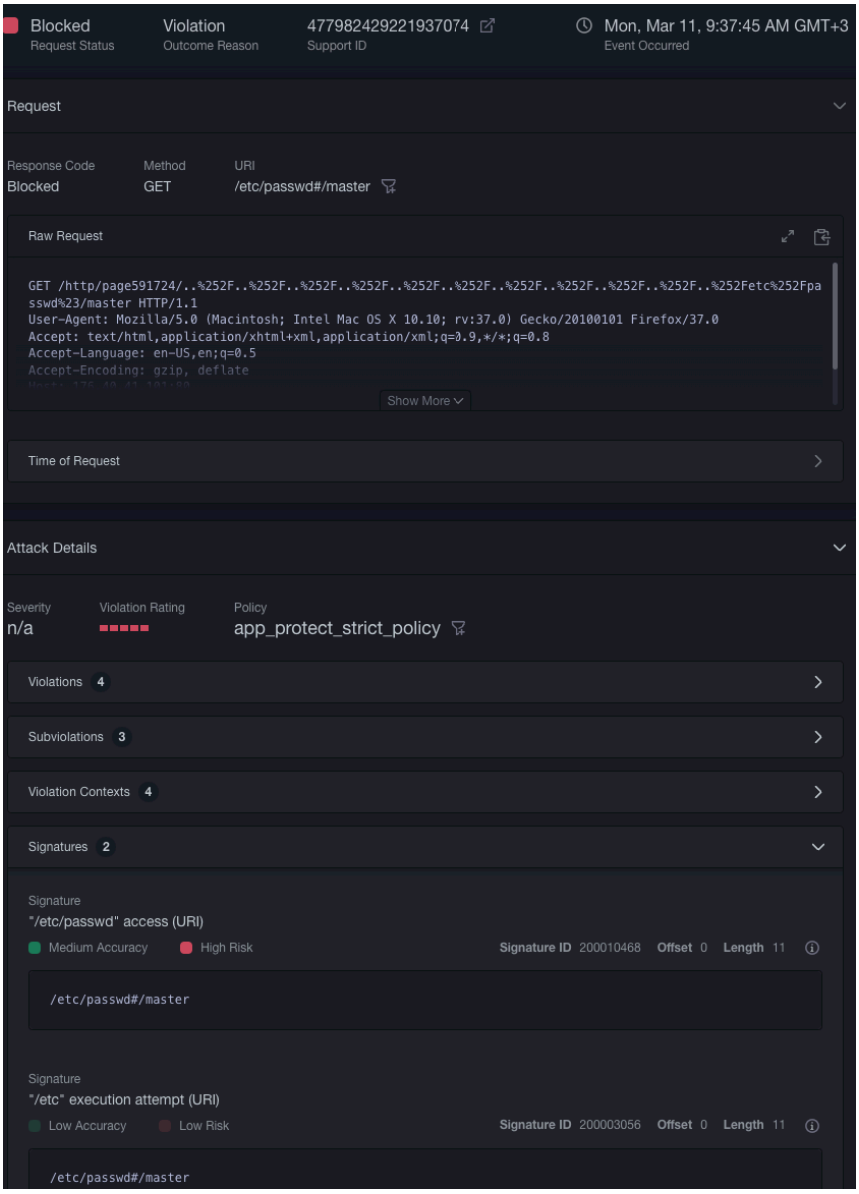
Bu üründe kullanılan raporlama tarafında F5-Nginx tarafından geliştirilmiş raporlama arabirimi bulunmaktadır.



Ayrıntılara biraz girdiğimizde;



Dashboard tarafında sade, güzel bir özet bizi karşılıyor.
Support ID ve Event Log larda da yeterli veri mevcut. Aynı F5 on-prem tarafında olduğu gibi ilgili support id aratılarak hızlıca ilgili “illegal log” kısmına erişim sağlanıyor.



F5 ile aynı veri tabanını kullanmakla birlikte kaynak kullanımı görünüme göre çok daha iyi optimize ediliyor.
Positive security kısmı kullanılmayacaksa, gui sizin için çok önemli değilse ve cli/manager üzerinden config editleyerek kullanım yapabilirseniz çok hızlı ve efektif bir şekilde sistemi devreye almak mümkün.

Aynı Waf güvenlik testi, F5-Nginx waf olarak kullanıldığında, 87 Skorunu almıştır. Ayrıntılı skor sonucu Ek1’de belirtilmiştir.

c. OWASP Coraza Web Application Firewall

Diğer incelediğimiz ürün ücretsiz olarak temin edilebilen bir ürün https://coraza.io/ adresinden erişim sağlayarak, hızlıca Linux üzerinde kurulumu gerçekleştirebilirsiniz.

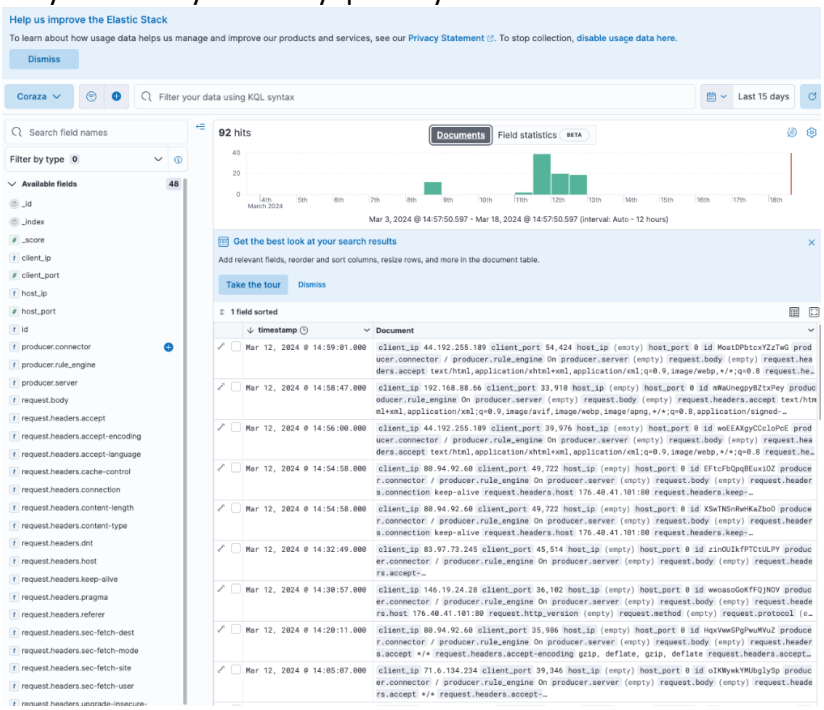
Politika olarak;

```
SecAction \
    "id:900990,\
    phase:1,\
    nolog,\
    pass,\
    t:none,\
    setvar:tx.crs_setup_version=400,\
    setvar:tx.inbound_anomaly_score_threshold=4,\
    setvar:tx.outbound_anomaly_score_threshold=3,\
    setvar:tx.blocking_paranoia_level=2"
```

seçeneklerini ile sistemi aktif olarak hızlıca devreye aldık.

Ürünün bir arayüzü yok, ancak raporlama tarafındaki oluşabilecek ihtiyacı, https://medium.com/@jptosso/oss-waf-stack-using-coraza-caddy-and-elastic-3a715dcbf2f2 adresindeki yönergeleri ekleyerek aktif edilebiliyor.

Arayüzde detaylı arama yapılabiliyor.



Aynı Waf güvenlik testini kullanarak, 89/100 puan gibi bir skora ürün ulaştı. Ayrıntılı skor sonucu Ek1'de belirtilmiştir.

3. Sonuç

Çalışmamızda incelediğimiz bütün ürünler sadece negative security tarafında önlem alınma hedefi doğrultusunda benzer performanslar ortaya koydular.

Günümüz çağında, sanal ve software sistemler de yüksek performans değerlerine ulaşabiliyorlar. Yapının düzgün kurgulanması, cihazların/yazılımların efektif kullanılması, güvenliğe bir bütün olarak bakıp, uygulama sunucularının genel segmentasyon ve güvenliği ön plana çıkararak ancak uygulama güvenliği tarafında bir sonuca varılabiliyor. Tüm bunların eş zamanlı yapılmadığı durumda, hangi ürün kullanılırsa kullanılsın, efektif bir uygulama güvenliğinden söz edilmesi çok da mümkün görünmüyor.

Saldırganlar öncelikle keşif çalışmaları yapar. Bu çalışmalar esnasında izler (port scan, bazı sql injection veya belli parametrelerle "etc/passwd" v.b.) bırakırlar. Çok basit anlamda tüm IPS sistemleri bu atakları tespit edip, ilgili IP'yi karantinaya alabilir. Bazı WAF sistemleri de karantinaya alabilir. Bu durumda atakların daha başlamadan kesilmesi sağlanabilir. Bu ve buna benzer onlarca örnek sayesinde güvenli altyapıların oluşturulması esasında zor değildir.

Positive security tarafında bir aksiyon alınacaksa, bunun zamansal olarak ciddi bir kaynak ve bilgi birikimine ihtiyaç duyulan bir süreç olduğu unutulmamalıdır. Bu işe kurumların ayıracak yeterli kaynağı yok ise dışarıdan danışmanlık hizmeti alınması daha doğru bir sonuca ulaştıracaktır.

Network security raporumuzu okumadıysanız ilgili kısımlara bakarak veya bizimle iletişime geçerek daha fazla bilgi elde edinebilirsiniz.

Ek1.Test Metodolojisi ve İlgili Veriler (Picus)

Test metodolojimizi puanlarken, Picus aracını kullandık.

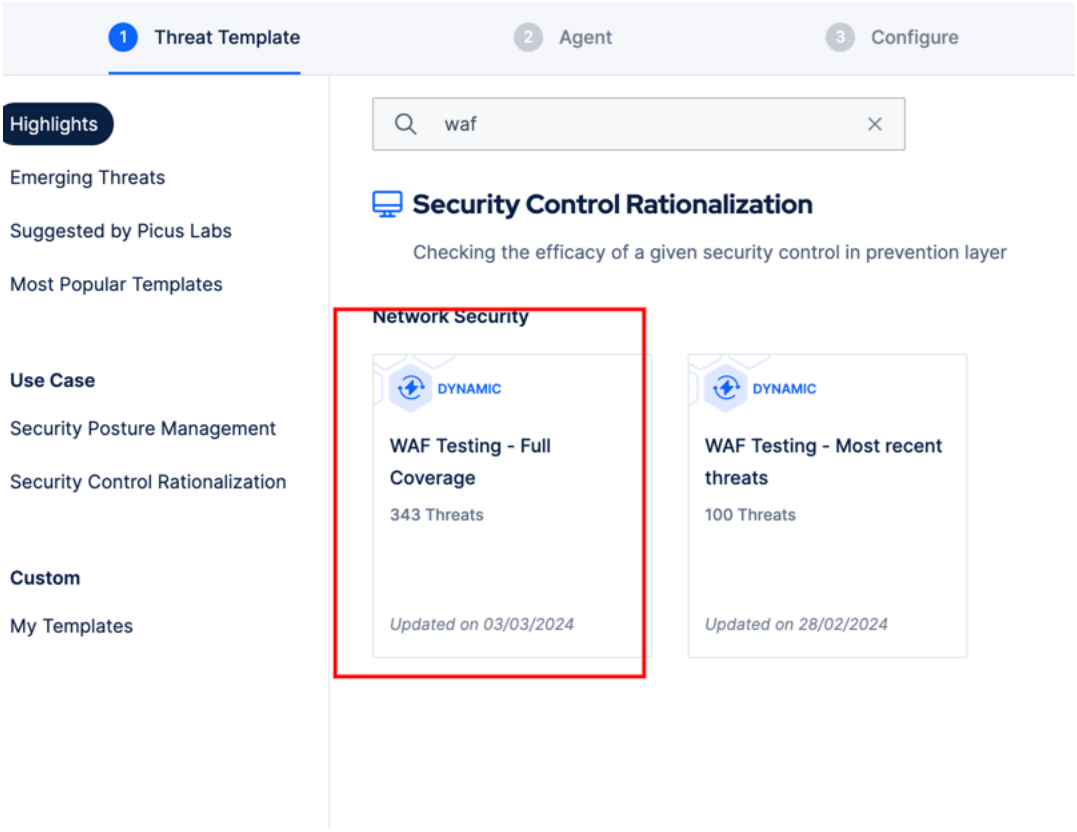
Kısaca bahsetmek gerekirse, Picus, siber güvenlik tehditlerine karşı koruma sağlanmasına yardımcı olan çeşitli ürün ve hizmetler sunar. Picus'un temel olarak çalışma prensibi, siber saldırıların gerçekleştirilmesi için kullanılan yöntemleri modelleyerek ve simüle ederek, organizasyonların savunma mekanizmalarını test etmektir.

Picus'un çalışma süreci genellikle şu adımları içerir:

1. **Gereksinimlerin Belirlenmesi:** İlk adım, müşterinin ihtiyaçlarını ve hedeflerini anlamaktır. Bu, belirli bir organizasyonun hangi tehditlere karşı savunma mekanizmalarını test etmek istediğini ve hangi tür simülasyonların yapılmasının gerektiğini belirlemeyi içerir.
2. **Simülasyon Senaryolarının Oluşturulması:** Picus, gerçek dünya saldırı senaryolarını modeller ve bu senaryoları müşterinin altyapısına uyacak şekilde uyarlar. Bu senaryolar, farklı saldırı vektörlerini ve taktiklerini içerebilir.
3. **Simülasyonların Yürütülmesi:** Picus, oluşturulan senaryoları kullanarak gerçek bir saldırıyı taklit eder. Bu, belirli saldırılarla ilişkilendirilmiş adımları, aşamaları ve saldırıları içerir. Bu simülasyonlar, organizasyonun mevcut güvenlik önlemlerini test etmek için gerçek zamanlı veri ve analiz kullanır.
4. **Sonuçların Değerlendirilmesi ve Raporlama:** Picus, simülasyon sonuçlarını detaylı bir şekilde analiz eder ve müşterilere güvenlik açıklarını, zayıflıkları ve iyileştirme önerilerini içeren kapsamlı raporlar sunar. Bu raporlar, organizasyonların güvenlik önlemlerini güçlendirmek için alabilecekleri adımları belirlemelerine yardımcı olur.

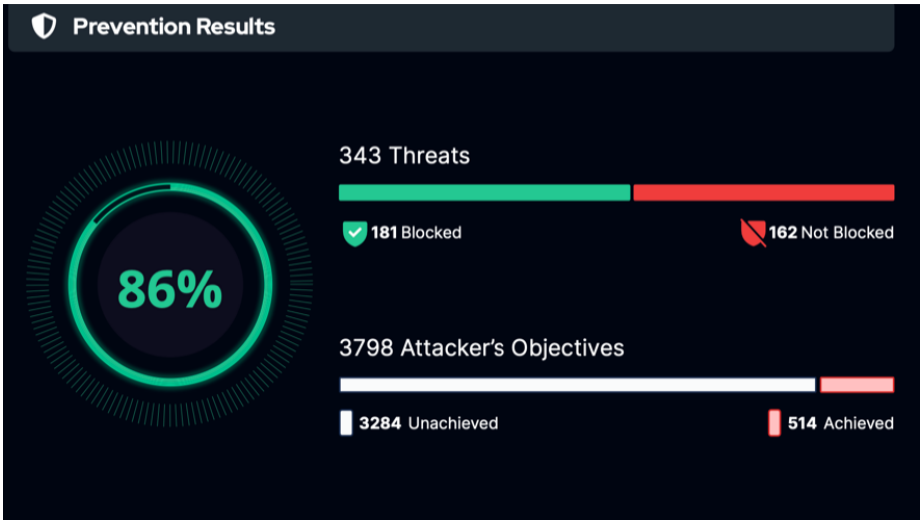
Picus'un bu çalışma prensibi, organizasyonların siber güvenlik savunmalarını sürekli olarak güçlendirmelerine ve güncel tehditlere karşı daha etkili bir şekilde korunmalarına yardımcı olur.

Bu bağlamda biz de Picus üzerinde var olan hazır template “WAF Testing - Full Coverage” isimli politikasını kullandık.



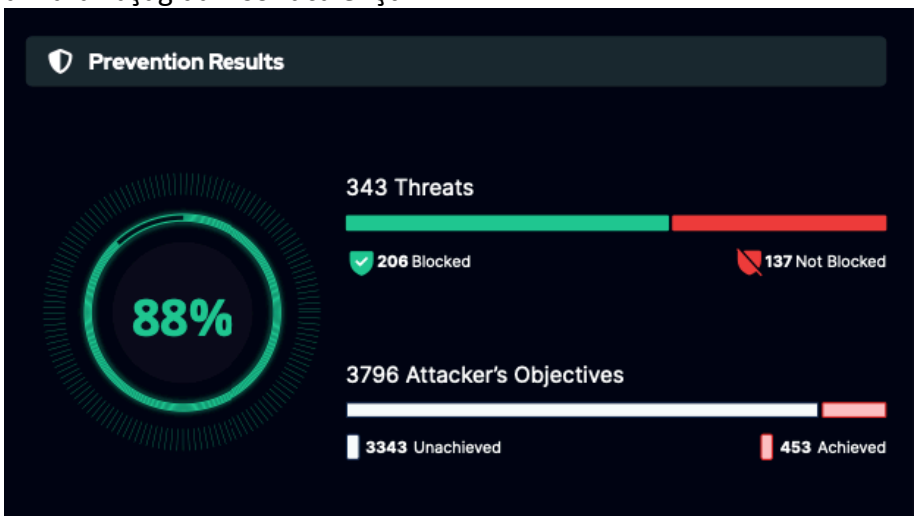
Raporda da belirttiğimiz gibi ulaştığımız sonuçlar benzerdi.

F5-Ltm cihazi üzerinde, Waf policy (negative security) aktif edilerek %86 gibi bir sonuca ulaşıldı.



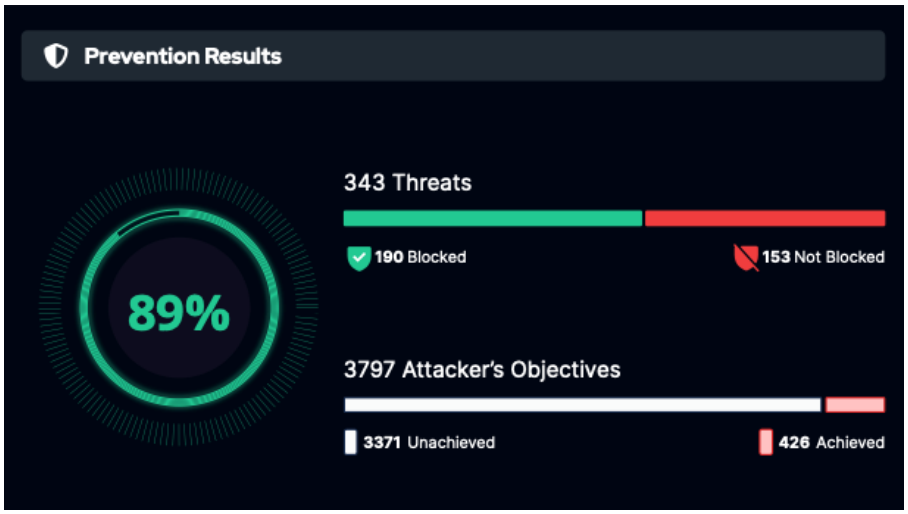
F5 Waf Test (Negative Security) Sonuç Özeti

Ubuntu üzerinde koşan Nginx+ yazılımı ile üzerinde hali hazırda gelen “NginxStrictPolicy.json” politikası kullanılarak aşağıdaki sonuca eriştik.



F5-Nginx Test (Negative Security) Sonuç Özeti

Son olarak OWASP Coraza Web Application Firewall ile de aşağıdaki skora eriştik.



Coraza Web Application Firewall Test (Negative Security) Sonuç Özeti