

CVE-2021-44228

Açıklama

Bu Güvenlik Uyarısı, Apache Log4j'deki bir uzaktan kod yürütme güvenlik açığı olan CVE-2021-44228'i ele alır. Saldırganlar kimlik doğrulama olmadan uzaktan kullanılabilir, yani bir kullanıcı adı ve parola gerekmeden bir ağ üzerinden bu zafiyet sömürülebilir.

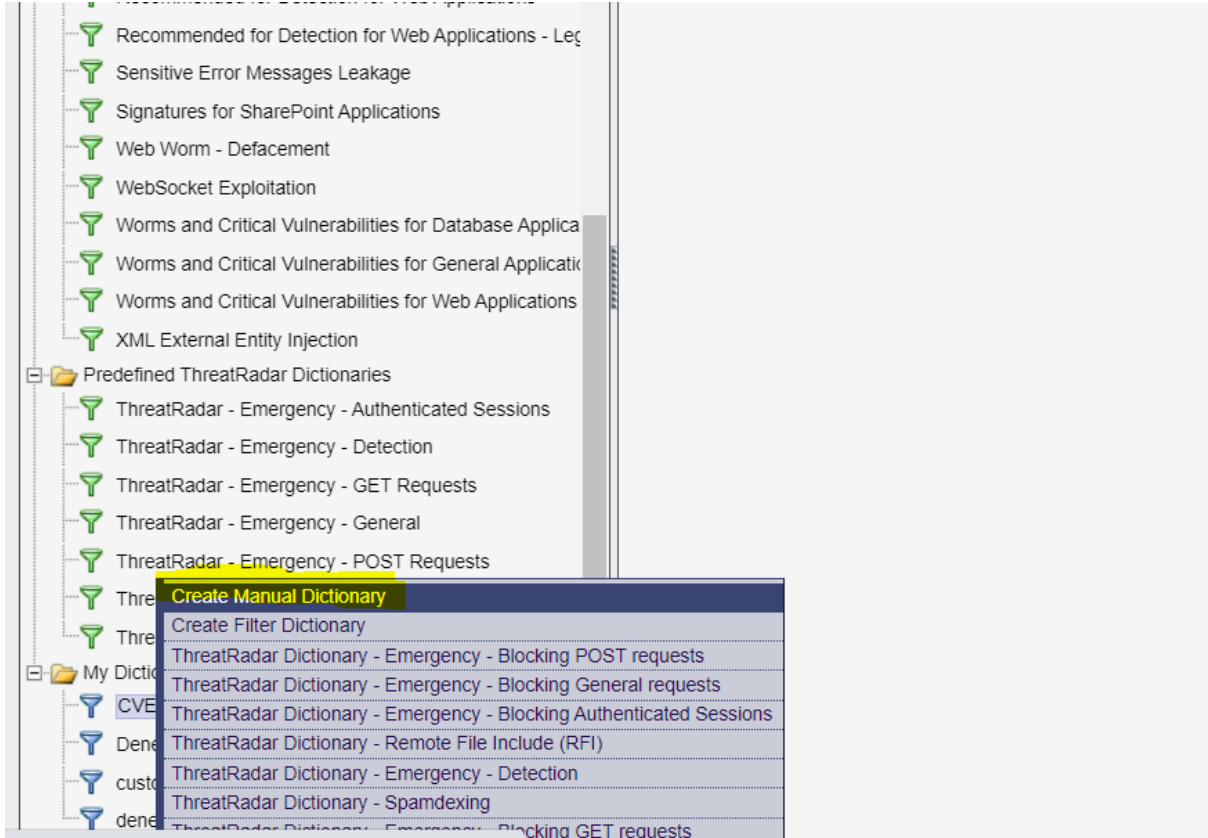
Önem Derecesi

Kritik

Imperva WAF için alınacak önlem

1. Custom Dictionary oluşturulması

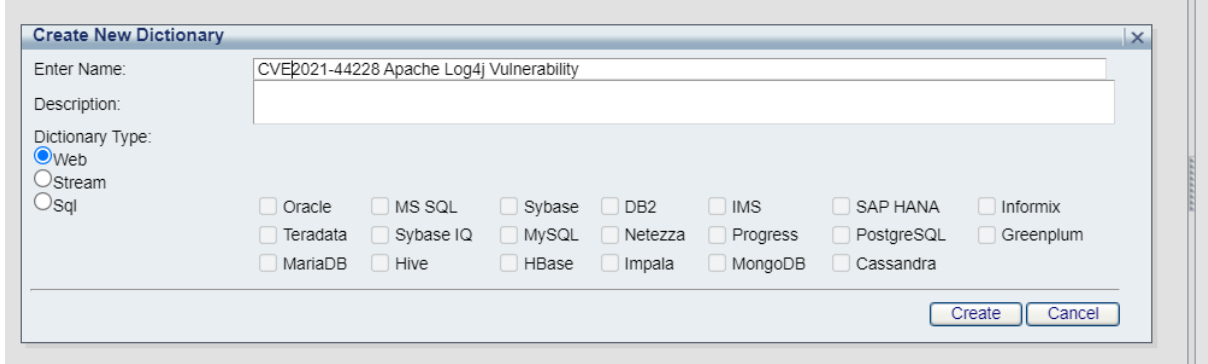
- Setup>Signitures sekmeleri takip edilir
- Sol panelde en altta bulunan my dictionaries sekmesine sağ tık yapılarak “create manuel dictionary” seçilir.



HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

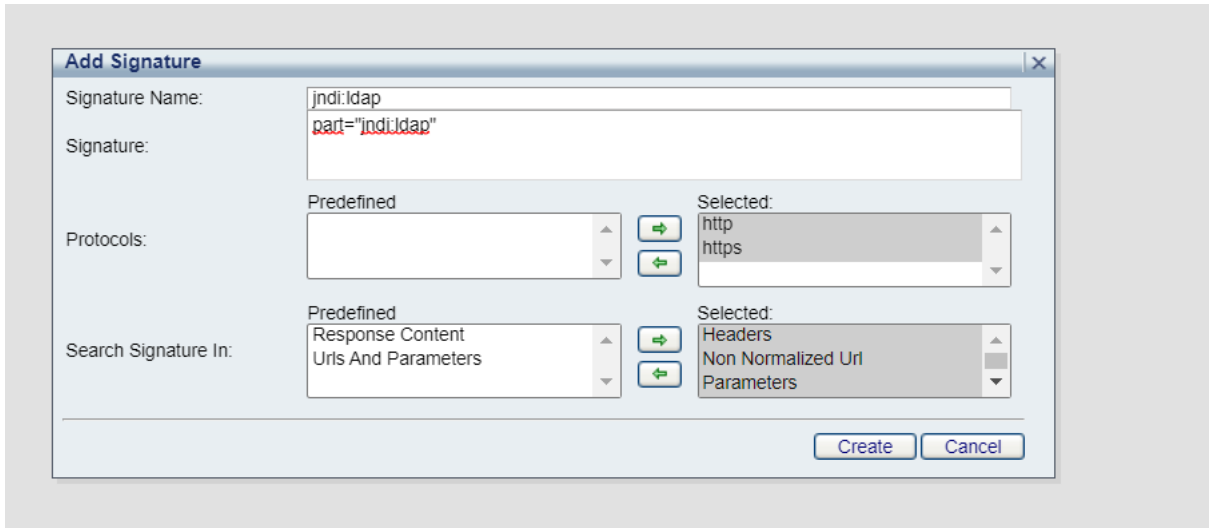
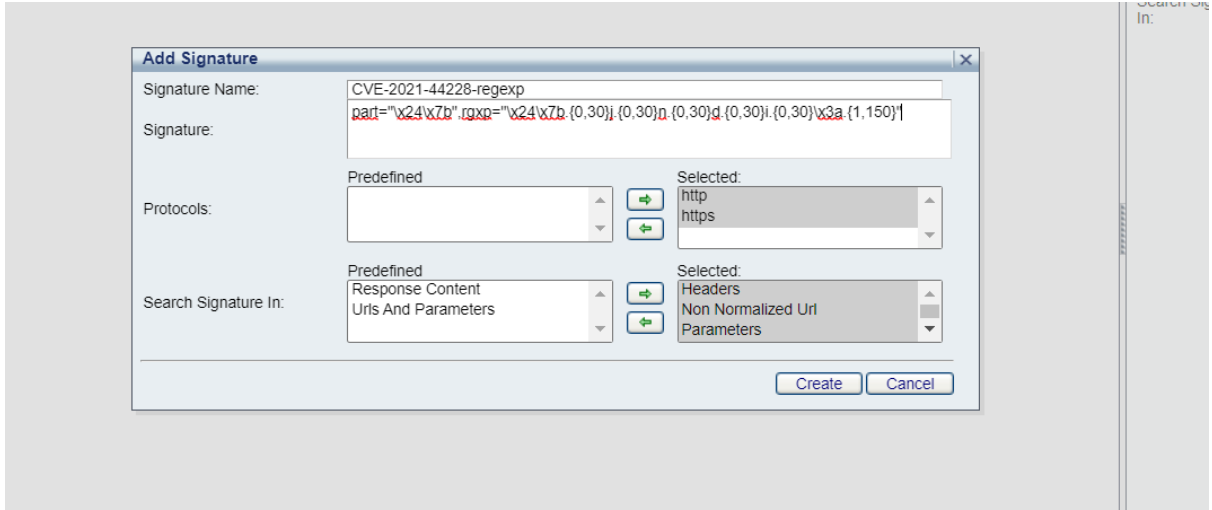
→ Açılan panelde ilgili zafiyetin ismi girilir ve type olarak web seçilir.



→ Create seçeneğine basıldıktan sonra dictionary oluşturulur.

→ Sonraki aşamada oluşturmuş olduğumuz dictionary içerisine zafiyet payloadlarında kullanılan “jndi:dns” , “jndi:ldap” , “jndi:rmi” ve CVE-2021-44228-regexp ismiyle 4 adet imza oluşturulur.

- Burada imza oluştururken “jndi:ldap” için signature part="jndi:ldap" şeklinde “jndi:dns” için part="jndi:dns" jndi:rmi için part="jndi:dns" şeklinde imza tanımı yazılmalıdır
- CVE-2021-44228-regexp imzası için ise part="\x24\x7b",rgxp="\x24\x7b.{0,30}j.{0,30}n.{0,30}d.{0,30}i.{0,30}\x3a.{1,150}" şeklinde regex yazılmalıdır
- Protocols olarak http ve https seçilmelidir.
- Search signature in kısmında ise Parameters,Request body,URL,Headers,Non-Normalized URL seçili olmalıdır.



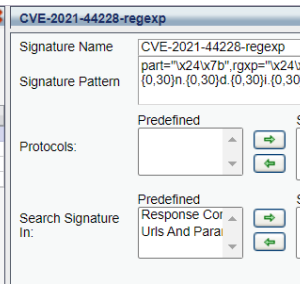
- Create butonu ile imza oluşturulur.
- Son görüntü aşağıdaki gibi olmalıdır.

CVE-2021-44228 Log4J Vulnerability - Manual, Web

Description:

Page 1 of 1

Name	Pattern	Protocol
CVE-2021-44228-regex	part=\"x24x7b\".rgxp=\"x24x7b.{0,30}.{0,30}n.{0,30}d.{0,30}i.{0,30}x3a.{1,150}\"	http, https
jndi:dns	part=\"jndi:dns\"	http, https
jndi:ldap	part=\"jndi:ldap\"	http, https
jndi:rmi	part=\"jndi:rmi\"	http, https



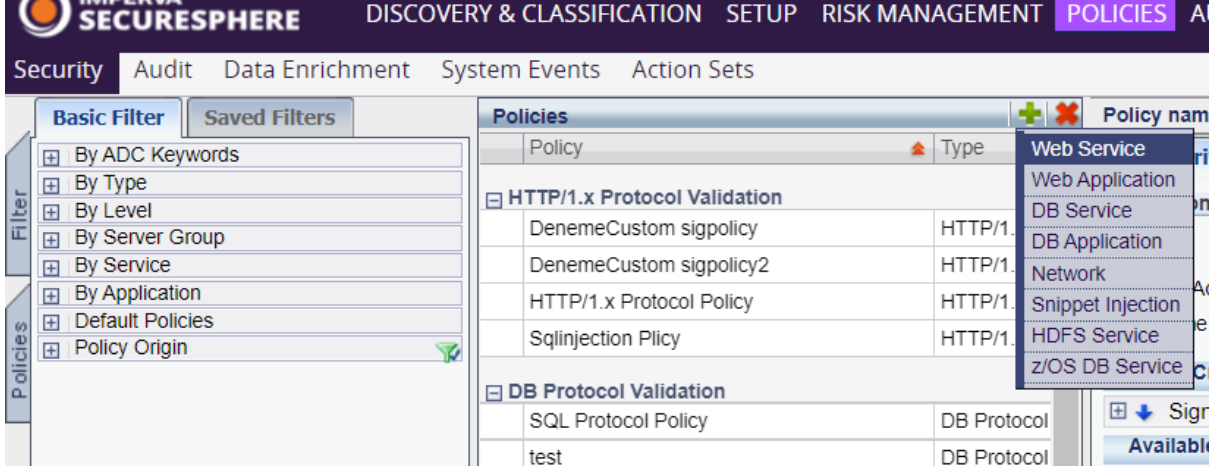
HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

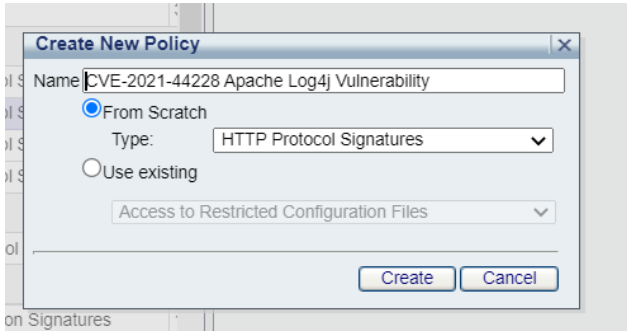
2. Custom Web Service politikası oluşturulması

→ Policies>Security sekmeleri takip edilir

→ + butonuna basılarak, seçenekler içinden web service seçilir.



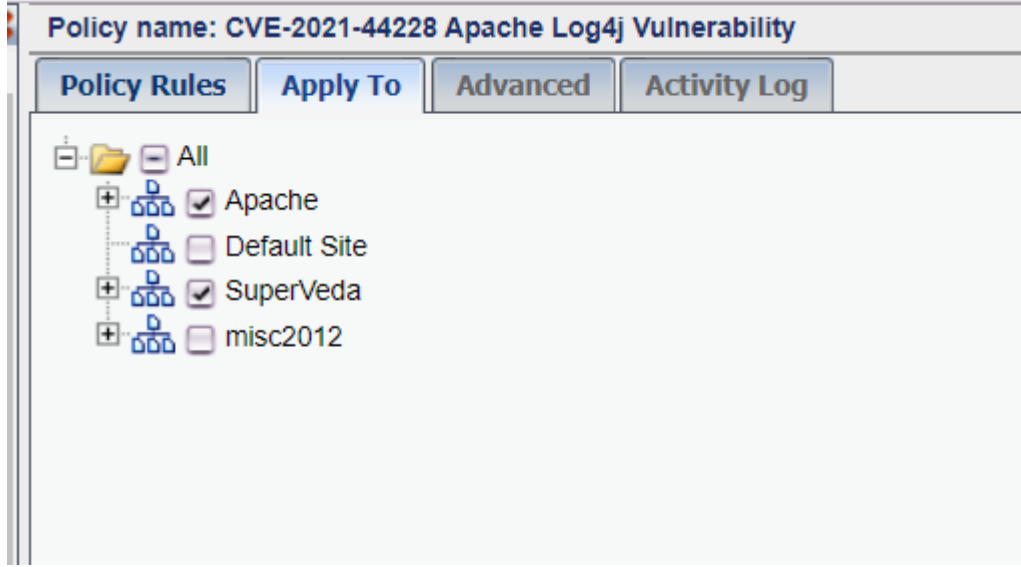
→ Açılan sekmede ilgili zafiyetin ismi yazılır ve type olarak http protocol signitures seçilir.



→ Policy Rules sekmesinde + butonuna basarak 1. Aşamada oluşturmuş olduğumuz dictionary seçilir. Son durum ekran görüntüsünün aynı olmalıdır. Yani Severity no alert ve action none olmalıdır.



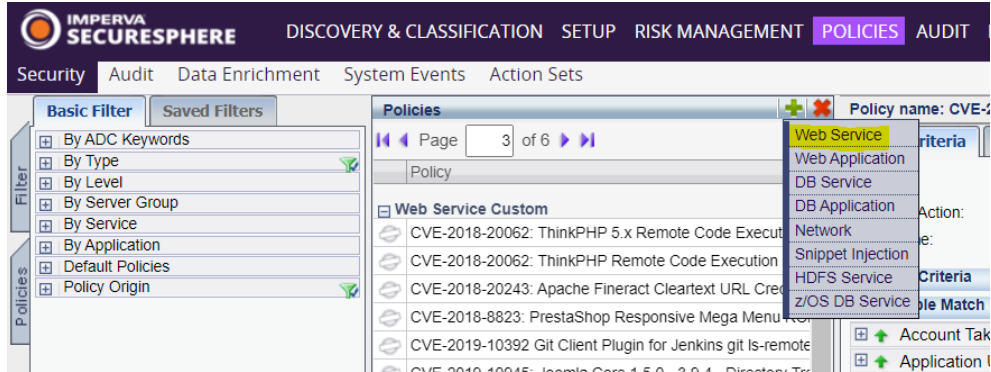
→ Değişiklikleri kayıt ettikten sonra, apply to sekmesinden ilgili servislere politika atanır.



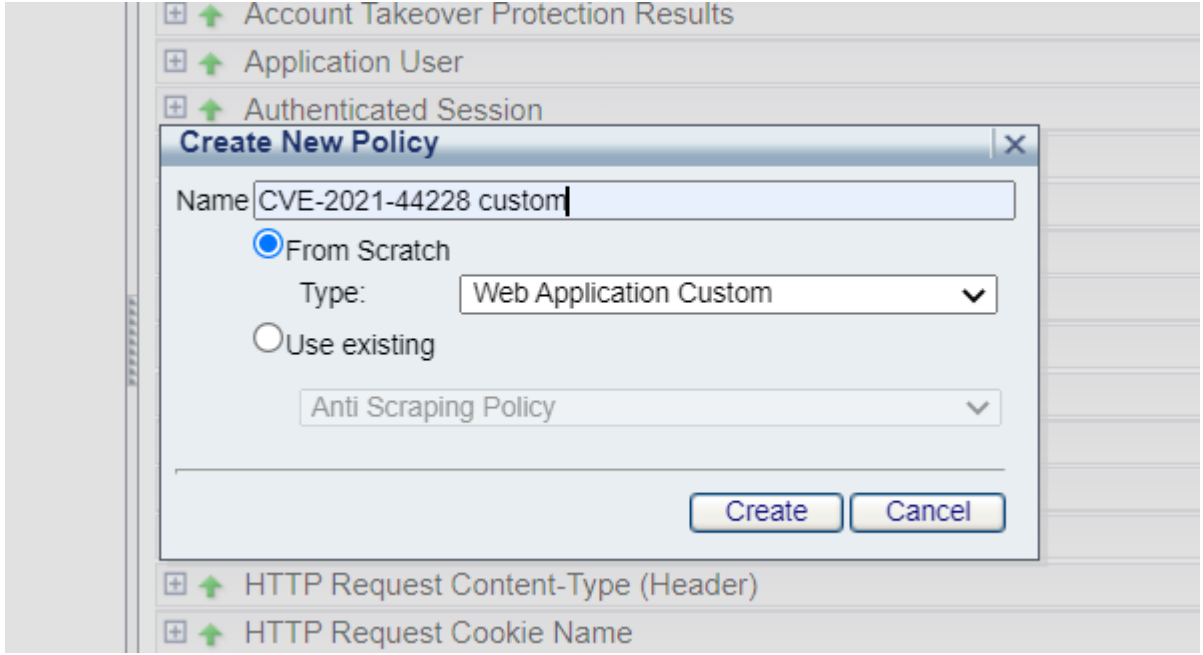
3. Web Servis custom politikası oluşturulması

→ Policies> Security sekmeleri takip edilir.

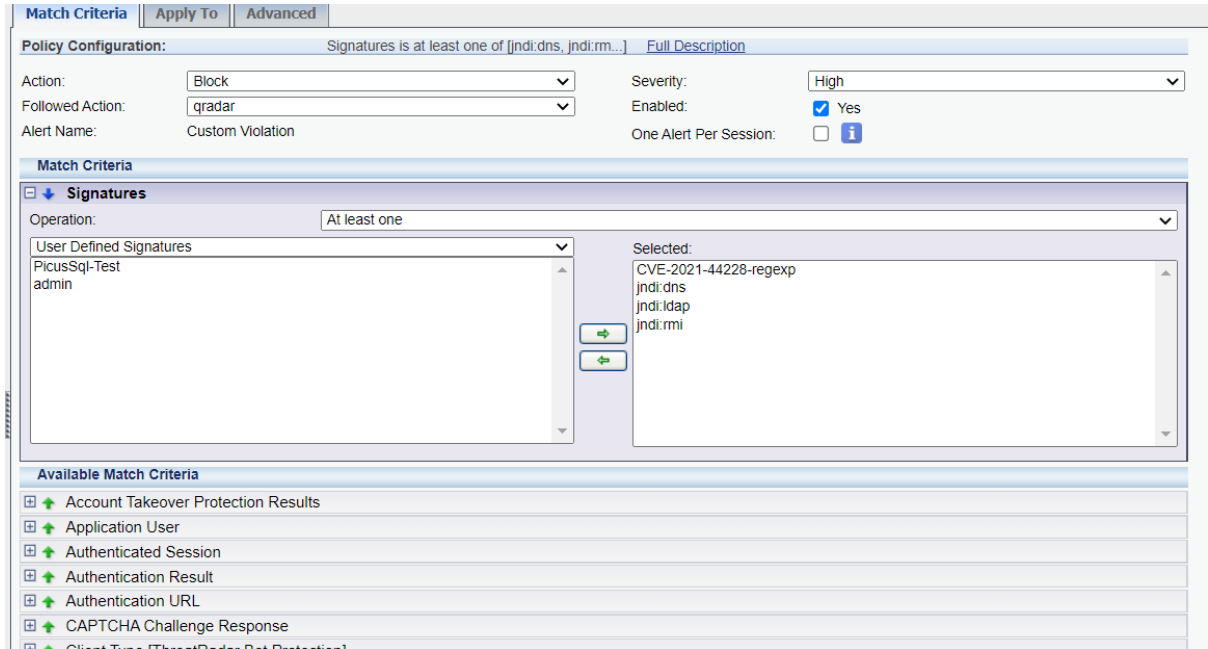
→ + butonuna basılarak, seçenekler içinden Web Service seçilir



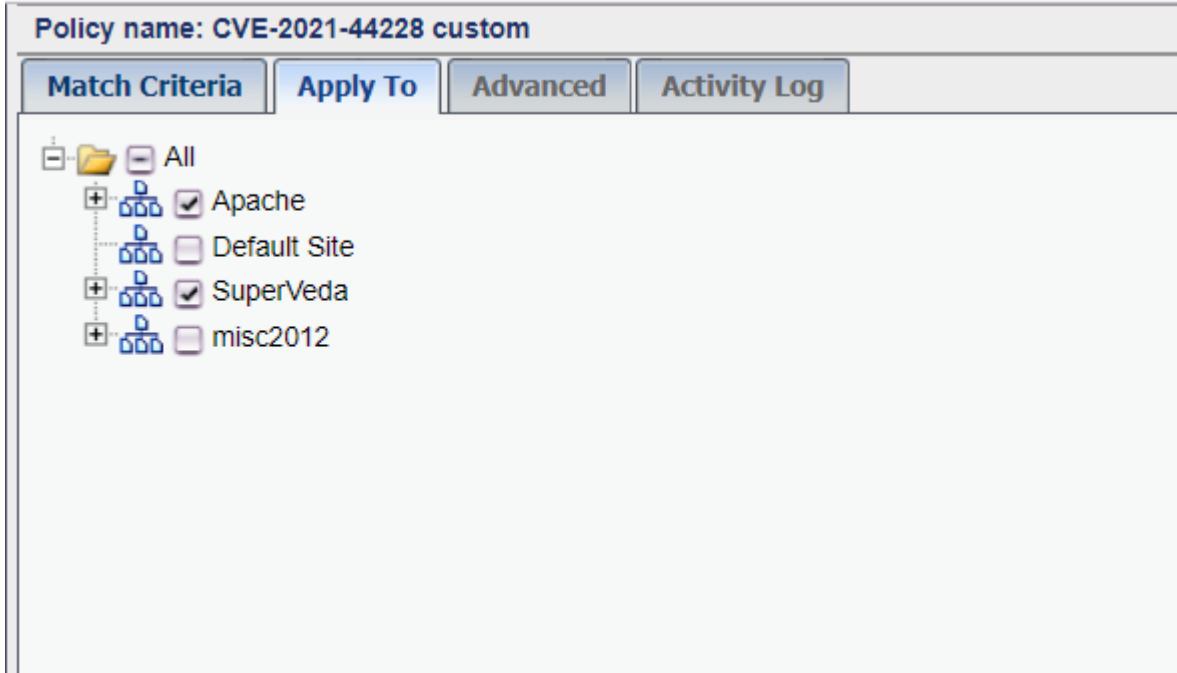
→ İlgili zafiyetin ismi oraya yazılır ve type olarak web service custom seçilir.



- Açılan panelde match criteria olarak signatures seçilir. Ve operations kısmında user defined signitures seçilir, daha sonrasında önceden oluşturmuş olduğumuz imzaları sol sekmeden, sağ(selected) sekmeye alınır. Oluşturmuş olduğumuz politikanın action'ı block, severitysi high olmalıdır.

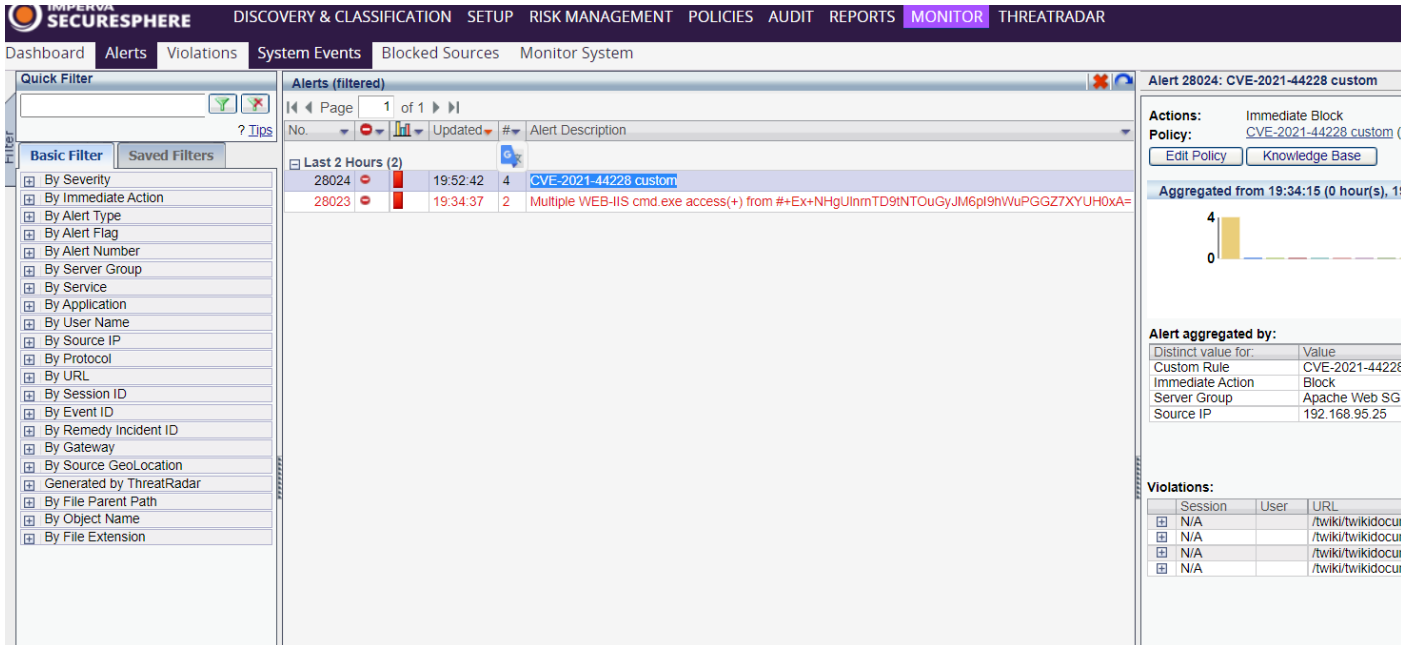


→ Apply to kısmında ilgili servisler seçilir.



4. Monitor

Bu zafiyeti sömürmeye yönelik bir atak gelirse Monitor>Alerts kısmından CVE-2021-44228 politikasının tetiklendiğini görebilirsiniz.



HİZMETE ÖZEL / Sadece İç Kullanım

BARİKAT İÇ KULLANIM

Referans Baęlantıları

<https://nvd.nist.gov/vuln/detail/CVE-2021-44228>

<https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability>