


Valhalla

Loki - signature based

Naxtron-systems.com/valhalla

Valhalla Rule Feeder



Valhalla, Loki ile aynı şirketin sunmuş olduğu bir ürün. Ücretsiz olarak güncel YARA kuralları almamızı sağlıyor. Valhalla'da güncel olarak +13000 Yara kuralı bulunmaktadır. Günlük Olarak Yara kuralları güncellenir. Get Access API key olmadan sadece DEMO API key ile gelen YARA kurallarını kullanabilirsiniz. Get Access API key abone olunan şirketlere sağlanmaktadır.

```
from valhallaAPI.valhalla import ValhallaAPI
```

```
import os.path
```

```
save_path = 'C:/Users/Pwnlab/Desktop/loki/signature-base/yara'
```

```
api = ValhallaAPI(api_key = "{api_key}")
```

```
save_path = api.get_rules_text()
```

```
with open('valhalla-rules.yar', 'w') as vh:
```

```
    vh.write(save_path)
```

Tüm bu işlemleri yaptıktan sonra Linux veya Windows tarafında bir crontab(cronjob) ekleyerek güncel kurallardan anlık olarak beslenebiliriz.

```
0 03 1-31 * * /usr/bin/python3 /home/loki/valhalla/Desktop/APIscript.py
```

Ayın her günü gece saat 03:00'da API kod betiğimiz çalışarak, /yara dizinin altına en güncel YARA kural setini yazdıracaktır.

NOT: Loki'de YARA kurallarının aynısı aynı dizine yazılmış olsa bile, algoritması sayesinde sadece bir tanesini çalıştıracaktır ve performans kaybının önüne geçecektir.

crontab.guru

IoC (Indicator of Compromise), bir olay incelendikten sonra o zararlı hakkında çıkartılan;

- IP adresleri
- Kötü amaçlı yazılım dosyaları
- MD5 Hash'leri
- Botnet vb. Komutları
- C2 URL & Domain

Ve daha fazlasından oluşur. IoC'lerin analistlere olay analizi sırasında büyük kolaylık sağlar. IoC'lerin amacını kısaca böyle açıklayabiliriz.



