VALHALLA

nextron systems

Supercharge Your Detection

Valhalla boosts your detection capabilities with the power of thousands of hand-crafted high-quality YARA rules.

Our team curates more than 8000 quality tested YARA rules in 6 different categories: APT, Hack Tools, Malware, Web Shells, Threat Hunting and Exploits. Valhalla's database grows by 1500 YARA rules per year.

With access to Valhalla, you can supercharge your detection by adding most of our highly successful THOR scanners' signatures to your own scan engines.

All rules are performance optimised and quality tested against Terabytes of goodware and other data.

Huge Curated Rule Set

Quality Tested

Rich Meta Data

Valhalla provides rich meta data that adds valuable context to each match, like a web reference, related threat group campaigns, hashes of samples for which the rule was initially created and a list of public samples on which the rule has matched so far.

Meta Data is Key


```
rule MAL_ZombieBoy_Malware_Gen_Feb19_1_RIDDC6 : EXE FILE MAL GEN {
   meta:
      description = "Detects ZombieBoy malware"
      author = "Florian Roth"
      reference = "https://www.alienvault.com/blogs/labs-research/zombieboy"
      date = "2019-02-05 15:47:31"
      score = 70
      customer = "x23"
      required_modules = "pe"
      minimum_yara = "3.0.0"
   strings:
      $x1 = "C:\\Users\\ZombieBoy\\" ascii
      $s1 = "C:\\Windows\\System32\\sys.exe" fullword ascii
      $s2 = "RookIE/1.0" fullword ascii
   condition:
      uint16 ( 0 ) == 0x5a4d and filesize < 200KB and (
         pe.imphash ( ) == "6a79728a09f4edda13797e5ae0ffa0f3" or
         1 of ( $x* ) or
         2 of them
      )
}
```

Each rule contains information about the required YARA version and modules to run that rule.

The API client allows you to retrieve only those rules that your product supports.

The rule's score and tags indicate its reliability and scope. Both can be used to select the perfect rule set for your application.

Smart API

The Python API allows you download the the subscribed categories as text or JSON object. It even has presets for well-known products that support YARA scanning like FireEye's appliances, Tenable, Tanium, CarbonBlack or Symantec MAA. It requires no more than 3 lines of code to retrieve the subscribed YARA rule set.

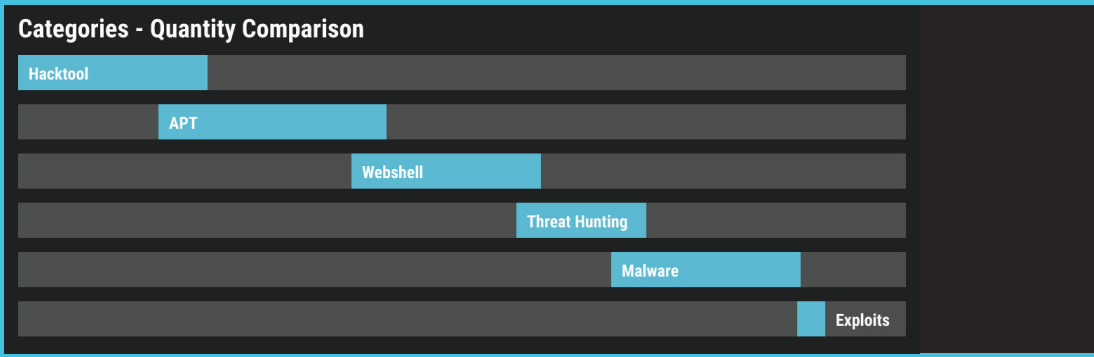
Flexible API

```python
from valhallaAPI.valhalla import ValhallaAPI

v = ValhallaAPI(api_key="Your API Key")
response = v.get_rules_text(product="FireEyeEX")
```

VALHALLA

Valhalla's rule set is divided into 6 categories based on tags that overlap



Strengths of the Set

APT

- High grade rules for malware and tools used by threat groups
- Based on public reports, our own undisclosed threat intel work, threat intel partners, threat exchanges and active incident response cases (mainly Europe, Asia and the Middle East)

Threat Hunting

- Generic rules / heuristic detection methods focus on methods and obfuscation instead of specific threats
- Highly effective in detecting new, yet unknown threats

Web Shells

- More than 1500 web shell rules
- Often very low Antivirus detection ratio
- One of the things most EDRs are unable to detect

Delivery

You can download the full subscribed set via web browser or use our public API client written in Python to get a customised rule set that fits your scan engine.

Subscription

We offer subscriptions for each of our rule set categories or the whole curated rule set.

Each subscription includes improvements, fixes and updates on the subscribed categories for 12 months.