VALHALLA

Nextron's detection rules. Incorporated into your security stack.

Keep your engine. Add the detection content Nextron's research team maintains for THOR: selected YARA and Sigma rules, in the tools you already run.

FILE & MEMORY DETECTION

YARA

Files · Memory · Artifacts

- **APT**
  Threat-actor tools and malware.
- **Hack tools**
  Offensive tools, output and traces.
- **Malware**
  Ransomware, stealers and more.
- **Web shells**
  Server-side backdoors and obfuscation.
- **Exploits**
  Exploit code and weaponized documents.

LOG & EVENT DETECTION

Sigma

Security monitoring · Threat hunting

- **Suspicious process chains**
  Web servers spawning shells or scripting engines.
- **PowerShell abuse**
  Malicious scripting and unusual execution.
- **Credential access**
  Behaviors associated with credential theft.

Telemetry → **Sigma** → **Detections**

Research-led

Threat intelligence, malware analysis and real incident response shape the detections.

Quality tested

YARA rules optimized for performance and tested against terabytes of goodware.

Actively maintained

New coverage, fewer false positives and refinements to existing rules. Sigma updates typically twice weekly.

nextron systems

We detect hackers.

500+ customers · 30+ countries · scanning tools recommended by security agencies

VALHALLA

Your tools. Expert detection content.

Maintained content, not just a rule format. Retrieve the right rules and build them into your workflow.

01

Select

Choose your feed and coverage. Filter YARA by tags, score, engine version or modules.

02

→ Retrieve

Use your API key in the browser, Python API or CLI. Automate downloads; proxy support included.

03

→ Deploy

Use YARA-capable endpoint, email or network tools. Deploy Sigma through compatible SIEM or log analytics tooling.

</> **YARA** Rule text / JSON | **Sigma** Rule ZIP / JSON

Context behind the match.

YARA

Trace the evidence

References, campaigns, initial sample hashes and known matching samples.

Choose your coverage

Subscribe to YARA categories or the full available set, with 12 months of fixes and updates. The private Sigma feed is curated by Nextron, separately from SigmaHQ.

SIGMA

Understand the behavior

Detection logic, references, log sources, severity levels and rule status.

Explore before subscribing

Download public demo rules and view current statistics in the portal. Selected private Sigma examples are available on request.

Public demos are not a trial of the private feeds.

valhalla.nextron-systems.com →

THOR-only YARA categories: Threat Hunting, Anomalies and Third Party.

Strengthen your detection stack.

info@nextron-systems.com
nextron-systems.com/valhalla