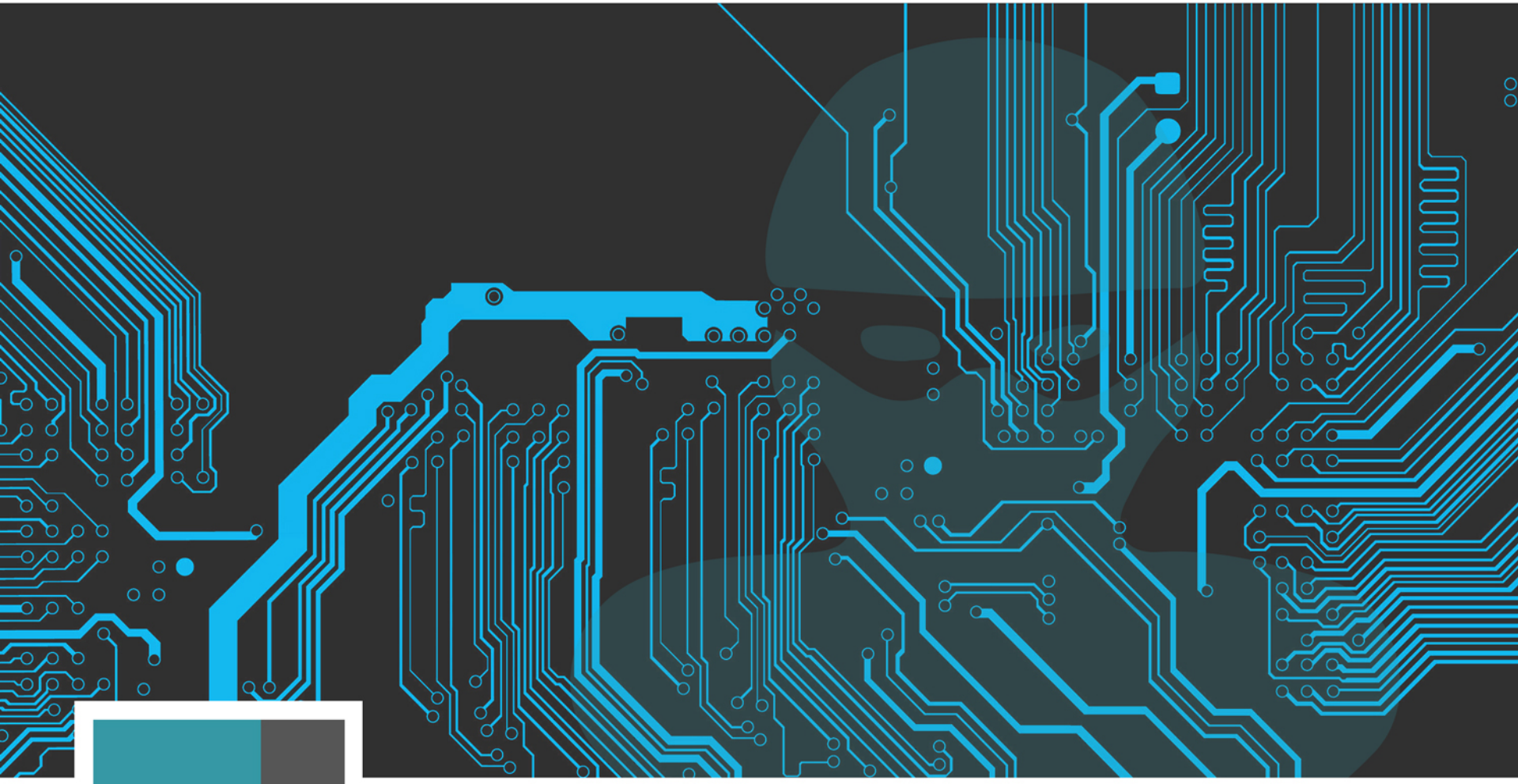
HvS consulting bsk consulting



THOR APT SCANNER

Revealing Attacker Activities and their Toolsets

What is THOR?

- Portable scanner for Windows systems
- Detects attacker toolsets and malicious activities
- Used for triage, incident response and live forensics
- Flexible due to open standards (YARA and STIX)

Focus on APT

- THOR focuses on hack tools and traces of hacker activity
- Although it is not an Antivirus it detects most Remote Access Trojans (RATs) used by common APT groups
- Big rule set with more than 3000 custom indicators on APT malware, hack tools, system file anomalies and suspicious log events

DETECT COMPROMISED SYSTEMS WITH A SINGLE

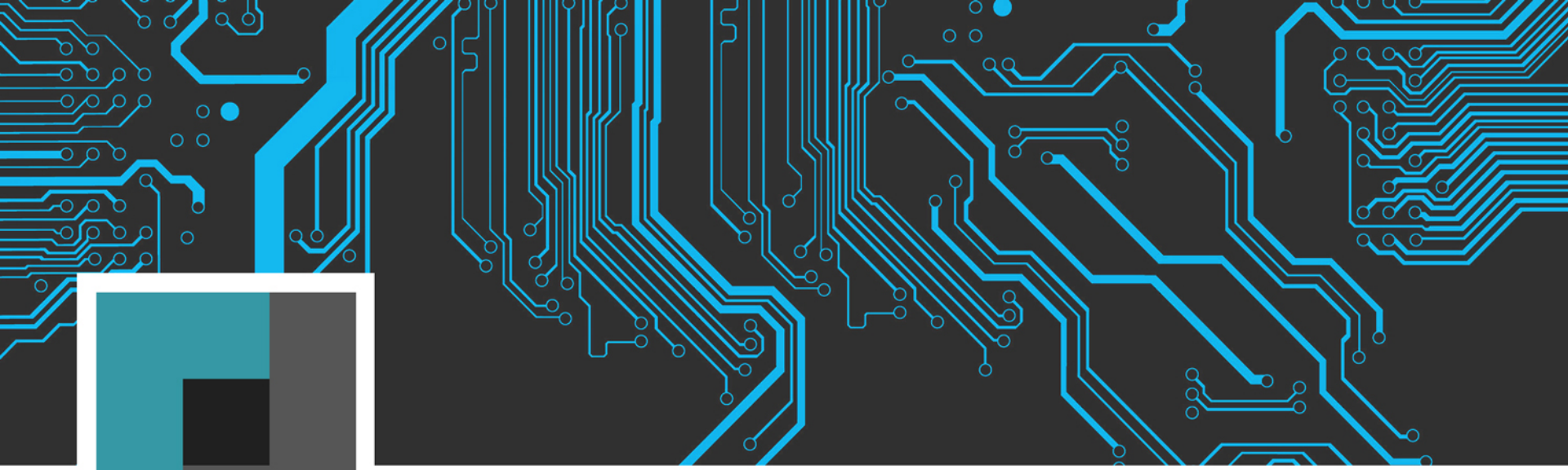
THOR SCAN

Reporting

- Simple TEXT log
- Easy to read HTML Reports
- SYSLOG output to collect log data during a distributed sweep (support for ArcSight's CEF)
- Free SPLUNK App

Why THOR?

1. Verify that you are not an APT victim
2. Scan suspicious or exposed systems easily
3. Add your custom signatures
4. Never put system stability at risk
5. Integrate the results into your SIEM infrastructure
6. Benefit from our secure indicator sharing program
7. Receive free signature updates



Learn more

Web

http://www.bsk-consulting.de/apt-scanner-thor/

https://www.is-fox.de/apt-scanner-gegen-angreifer-im-netzwerk.aspx

Twitter

https://twitter.com/thor_irs

Blog

http://www.bsk-consulting.de/category/thor-2/