PRODUCT BRIEF

Nimbus Threat Monitor

No-cost Threat Detection for ISPs and Hosting Providers

TEAM CYMRU

You are critical to delivering online access and services to the world. Yet, you may lack the advanced threat detection solutions or the human resources necessary to effectively defend your networks and prevent malicious abuse of your infrastructure. Unchecked cyber threats drive down your quality of service and jeopardize your customers, which can lead to lost revenue and the potential for regulatory enforcement actions…not to mention the cost of bandwidth wasted by bots and unauthorized proxies.

Many companies pay for our IP Reputation data.

Nimbus partners don't.

Founded by Internet Engineers, Team Cymru uses the same collaboration model that built the Internet to address threats. By joining us in making the internet a safer place, you will receive a purpose-built threat detection solution, created to auto-correlate your network flows with the same IP reputation data that powers many well-known cyber security solutions.

Automated Threat Detection
Powered by Pure Signal™

- Quickly identify compromised assets in near-real time.
- See who is draining your bandwidth for malicious purposes,
- Easily prioritize your remediation efforts.
- Reduce costs, overhead and your brand, while keeping the internet safer.
- Protect your clients.

World-class IP Reputation Feed

Automatic correlation of your network flows with Team Cymru IP Reputation data.

Near-Real-Time Threat Summary

Quickly identify the most critical compromises of your assets and those of your clients.

Incident Responders Report

Get a daily report of your remediation priorities.

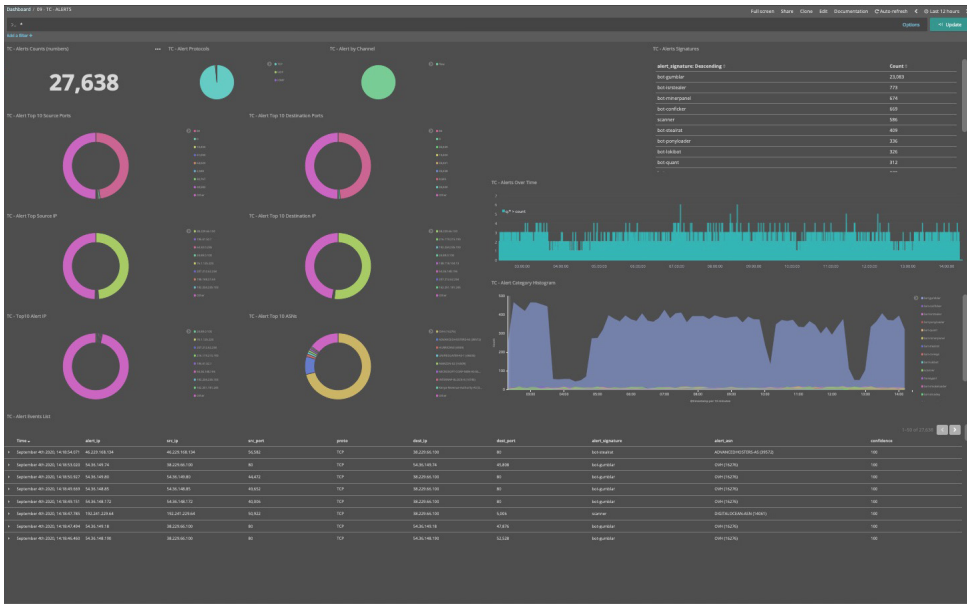
"The Nimbus tool is unique and essential to our CSIRT, because it gives us a detailed view of malicious activity (botnets, controllers) on our backbone."

- Francisco Badaró, Telecommunications and Training Manager, ITS Brasil

outreach@cymru.com

Nimbus Threat Monitor: Detailed views of malicious activity.

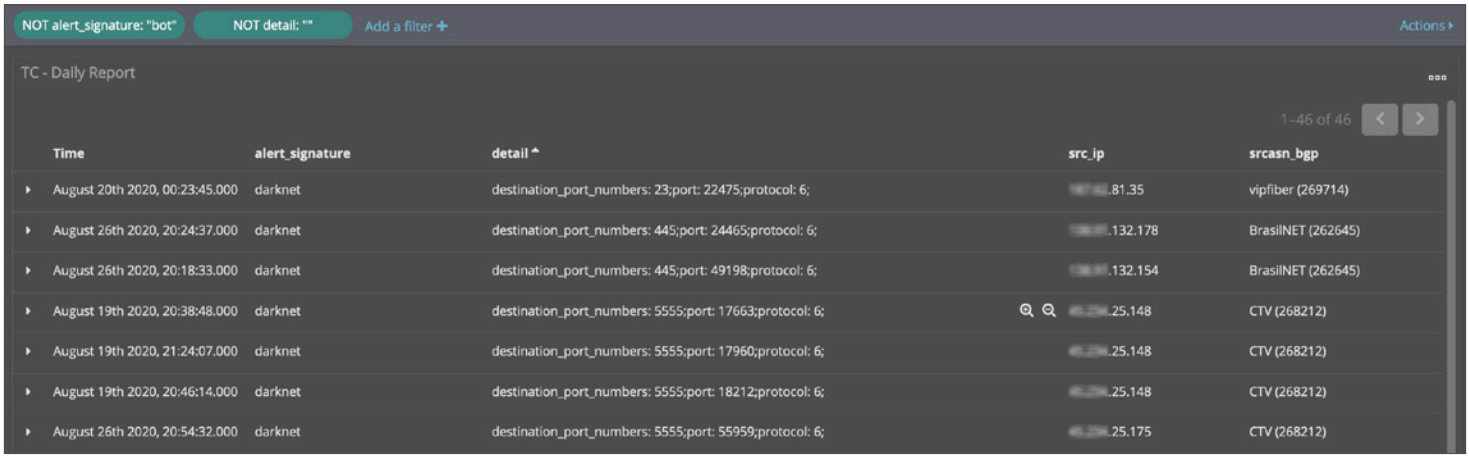
Harness the power of Kibana to create customized dashboards.



Key Features

- Near-real-time threat detection, powered by the world's most comprehensive IP Reputation data.
- Matches your network flows against over 7,000,000 indicators that are updated hourly.
- Customized filtering, allows you isolate malicious activity by type, network address ranges and more.
  - 18 alert filters
  - 31 network statistics filters
- SOC dashboard provides an at-a-glance view of top cyber threats and associated details.
- A daily report informs you of your remediation priorities.

Receive a daily remediation to-do list, prioritized by criticality.



Time	alert_signature	detail	src_ip	srcasn_bgp
August 20th 2020, 00:23:45.000	darknet	destination_port_numbers: 23;port: 22475;protocol: 6;	[redacted].81.35	vipfiber (269714)
August 26th 2020, 20:24:37.000	darknet	destination_port_numbers: 445;port: 24465;protocol: 6;	[redacted].132.178	BrasilNET (262645)
August 26th 2020, 20:18:33.000	darknet	destination_port_numbers: 445;port: 49198;protocol: 6;	[redacted].132.154	BrasilNET (262645)
August 19th 2020, 20:38:48.000	darknet	destination_port_numbers: 5555;port: 17663;protocol: 6;	[redacted].25.148	CTV (268212)
August 19th 2020, 21:24:07.000	darknet	destination_port_numbers: 5555;port: 17960;protocol: 6;	[redacted].25.148	CTV (268212)
August 19th 2020, 20:46:14.000	darknet	destination_port_numbers: 5555;port: 18212;protocol: 6;	[redacted].25.148	CTV (268212)
August 26th 2020, 20:54:32.000	darknet	destination_port_numbers: 5555;port: 55959;protocol: 6;	[redacted].25.175	CTV (268212)

CONTACT US
tel: +1 847-378-3300
fax: +1 407-878-7833
sales@cymru.com

EMERGENCY CONTACT
+1 847-378-3301
support@cymru.com

TEAM CYMRU