Signal Sciences

Signal Sciences NLX

Leverage the power of our Network Learning Exchange to see and stop known threats before they harm your business

SUMMARY

Signal Sciences NLX recognizes attack patterns across our customer network to proactively alert and defend all web applications and APIs.

Attackers targeting your web applications today are using automation tools to probe many sites with little effort. Advanced warning of malicious activity elsewhere in the Signal Sciences network among peer companies is critical to keeping attackers from stealing your business and customer data. Signal Sciences Cloud Engine collects anonymized attack data from tens of thousands of our distributed software agents, and learns by correlating patterns from the data to form Signal Sciences Network Learning Exchange (NLX). NLX provides early notice of threats that gives your teams visibility and time to better defend your web applications and services.

Powered by intelligence derived from Signal Sciences' network of customers large and small—spanning leading media, technology, finance, and healthcare verticals—Signal Sciences NLX shares confirmed malicious IP sources within Signal Sciences Console, alerting you to suspicious actors before they are a threat to your sites.

Accurate Intelligence From Trusted Sources

Signal Sciences NLX is a trusted, accurate IP reputation feed based on confirmed malicious activity collected from Signal Sciences customers—95% of whom are running in blocking mode to stop attacks. Because of our accurate detections, NLX is uniquely able to recognize attack patterns and identify potential threats before they become malicious on other sites protected by Signal Sciences.

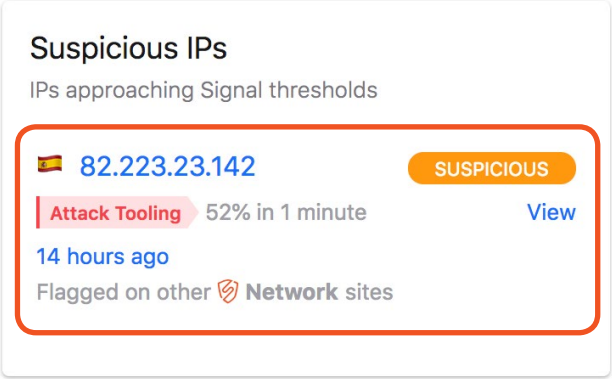
Enriched Agent Intelligence Without False Positives

Unlike other crowd-sourced threat intelligence services, Signal Sciences NLX doesn't send generic signatures that can cause false positives if implemented, but instead alerts on confirmed malicious sources detected via our proprietary SmartParse technology. SmartParse leverages the intelligence and analysis of Signal Sciences NLX

to automatically enrich its dynamic, application specific detections made at the agent, providing not only advanced warning, but ongoing, augmented intelligence for enhanced protection of your sites.

Leveraging Power Rules for Automated Blocking

The Network Signal can be used to trigger alerting and blocking actions via Power Rules, allowing you to automate actions based on NLX as a trusted source.



Stronger Together

With Signal Sciences NLX, you gain the strength of Signal Sciences' protected customer network, made up of leading brands accounting for over 150 billion production weekly requests. With a powerful, growing customer base, Signal Sciences is powering early detection of web application attacks on a global scale that enables superior detection and protection to keep your company and customer data safe.

NLX is included with your Signal Sciences license.

Any App

Infrastructure support

kubernetes, IBM Cloud, Google Cloud, aws, Pivotal

VIEW ALL >

Web Server and Language Support

NGINX, Microsoft IIS, APACHE

VIEW ALL >

Gateways and Proxies

section.io, Kong

Any Attack Type

OWASP Top 10

Application DoS

Brute force attacks

Account abuse and misuse

Request rate limiting

Account takeover attacks

Bad bots

Virtual patching

Any DevOps Toolchain

slack, HipChat

DATADOG, VictorOps

pagerduty, splunk>

elastic, ArcSight

Radar

Generic webhooks

Any custom tools via a full RESTful/ JSON API