Musubu

Bulk IP Address Info + Built-In Threat Intelligence

The operational IT and security departments of any organization need regular, easy access to bulk IP Address information, including geolocation, ASN, hostname, and company information for a myriad of daily uses (e.g., the development of applications, customer targeting, billing, command and control, network management, cybersecurity, and much more).

While there are services to look up data associated with an IP address, there's no API service that provides all the information your apps and operations need AND that tells you which IP addresses may have associated cybersecurity risks that affect your entire organization.

The lack of this type of coordinated service makes it harder to regularly identify risks and thus know how and when to respond to potential threats. It also splits out tasks that could otherwise be effectively combined into one operation to "kill two birds with one stone," making your daily routines more efficient – and more secure.

That's what Musubu achieves. Here's how it works.

Musubu meets a need for API-based IP address information and adds a security element to it.

Get IP *and* cyber threat data in one API call.

Get all the IP address data your apps need, like geolocation, carrier info, and company, along with a simultaneous overall threat score for each IP along with the type and volume of cyber threats.

Musubu easily allows users programmatic access to needed IP address info in bulk (or via our user interface) as well as characterizations of any IPs you return that have identified cybersecurity risks. It further characterizes what those risks may be, while also prioritizing them so you can attack the most significant problems first.

In short, Musubu adds a network dimension to threat intelligence that can enhance risk scoring and prioritization while helping organizations to better understand the IP addresses interacting with their networks.

It's utility + cybersecurity.

This paper will address how Musubu works, what it achieves, and what kinds of innovative use-cases become possible when this kind of IP and cyber data becomes readily available at a click.

When you query for one or a set of IP addresses, Musubu returns register info plus geolocation. Then, it goes a step further to add a security element and note if the IP address has been seen in relation to malicious activity like ransomware.

Organizations often lack key data to contextualize the network activity they observe, particularly when it comes to IP addresses. That can leave them with unanswered questions about core IP data needs, as well as unable to accurately assess serious cyber threat questions such as:

"Threat Potential" Score	How at-risk is each IP address?
Malicious Activity Indicators	Is there bad activity going on at the network level?
Types of Malicious Activity	What suspect activity has been seen, e.g., phishing, ransomware, etc.?
Extent of Malicious Activity	How much bad activity is happening?
ISP Demographic Data	What is the ISP name, network type, and group? What other information can be provided?
Ownership & Geolocation Information	Where in the world is this ISP, and whose is it?

By assessing network level information, users can more fully contextualize IP data.

Add a network dimension to IP address data.

Musubu incorporates information about the types of activities an entire network engages in, as well as geographical data that can pinpoint activity originating in regions known to be supportive of criminal activity.

Most threat intelligence tools will score IP addresses according to risk, leaving departments drowning in spreadsheets of IP addresses, yet still potentially vulnerable to malicious IP addresses that have never shown up on any watchlist.

Given that the internet is a series of interconnected networks, it makes sense to consider the totality of the network from which the IP address originates.

For this reason, Musubu is network-centric, a focus that enables the tool to more fully characterize the activity – and any potential malicious actors – operating on the edges of your network.

In addition to providing core IP Address info in bulk for your applications and operations, Musubu's API data elements simultaneously help with other key network monitoring and cybersecurity tasks by providing data points like those enumerated in the figure on the next page.

Filter out irrelevant data, increase analyst efficiency

Get all the IP address data your apps need, like geolocation, carrier info, and company, along with a simultaneous overall threat score for each IP along with the type and volume of cyber threats.

This enriched profile of the IP can significantly reduce false positives.

A false positive is an error in data reporting in which an IP is incorrectly identified as a potential threat entity.

Identifying these unnecessary alerts is critical in today's environment. When nearly half of SecOps managers see more than 5,000 alerts per day, genuinely actionable information can easily get lost in the noise.[i] Half or more of those alerts turn out to be false positives – 52%, according to one study[ii] – and Ponemon reports that companies spend an average of $1.27 million annually and 395 hours per week chasing down false positives.[iii]

Through "vetted source" analysis and machine learning analytics, Musubu has demonstrated a 40 – 75% reduction in false positives, thus providing a greatly enhanced ability to quickly filter out irrelevant data and increase analyst efficiency.

Instead of the traditional single index model used to determine "probability of badness," the Musubu score is based on three separate scoring indexes: previous observations, the imminent threat posed by past observations, and the network environment itself.

Musubu output displayed in the API results

VERBOSE OUTPUT	
ipaddress	IPv4 address in 4-octet dot notation, from 0.0.0.0 to 255.255.255.255
ipint	IPv4 address as 8 byte integer representation. Integer 0-4294967295.
threat_potential_score_pct	Numeric threat score. Integer 0-100.
threat_classification	Overall characterization of threat. String, with one of the following values: High Medium Low Nuisance
blacklist_class	String, with one of the following values: apache blacklisted botnet botnetcnc bruteforce compromised ftp http imap mail malware phishing ransomware shunned sips ssh tor worm zeus
blacklist_class_cnt	Count of distinct sources which have identified the address as malicious. Integer.
blacklist_network_neighbors	Count of addresses present on the same subnet which have been identified as malicious. Integer.
blacklist_observations	Count of observations in the last 90 days. Integer.
country	Two character country designation based on ISO 3166-1 alpha-2. String.
stateprov	State or province. String.
district	String.
city	String.
zipcode	String.
latitude	Latitude. Float.
longitude	Longitude. Float.
timezone_offset	Timezone offset in hours. Float.
timezone_name	String.
ispname	Internet Service Provider (ISP) or associated organization. String, alphanumeric and punctuation.
network_type	The service classification for the associated network. String, with one of the following values: ACADEMIA (universities, schools, labs, and institutes) BROADBAND (residential and small business) CDN (commercial, P2P, and free content delivery networks) CLOUDHOSTING (cloud and web hosting environments) ENTERTAINMENT (music, TV, video sharing, and gaming) FILESHARING (commercial and free) GOVERNMENT (federal, state & local, and foreign governments) HEALTHCARE (commercial) INTERNETAUTHORITIES (government, non-profit, and international authorities) INTERNETSECURITY (commercial internet security firms) SEARCHENGINE (commercial) SOCIALNETWORKING (commercial social networking sites) SOFTWAREDOWNLOADS (commercial and free) CRYPTOCURRENCY NODES (public and hidden TOR services) COUNTRY
network_group	String.
network_name	String, alphanumeric plus punctuation.

Musubu's API is quick and simple, enabling users to build better sites and apps with our IP data.

Work faster with thorough IP data available at a click.

"Musubu integration with our SIEM reduces time to action by as much as 25% relying on proofed information. Our cybersecurity threat hunters are able to action security events with a higher degree of confidence and focus more on containment and mitigation actions rather than context building activities."

– Musubu user

API results produce a significant amount of valuable data, including:

1 threat_potential_score_pct	Numeric threat score between 0-100. The Score is calculated using "blacklist class", "blacklist neighbors", number of recent observations and country of origin.
2 threat_classification	Classification derived from "threat potential score pct" and indicated as: • High – Threat score >70 • Medium – Threat score from >40 but <70 • Low – Threat score <20 • Nuisance – Threat score <40
3 blacklist_class	Field classifying the specific threat vector that has been identified. Contains one of the following values: apache, blacklisted, botnet, botnetcnc, brute force, compromised, ftp, http, imap, mail, malware, phishing, ransomware, shunned, sips, ssh, TOR, worm, zeus.
4 blacklist_class_cnt	Field providing the number of sources which have identified the address as malicious.
5 blacklist_network_neighbors	Field providing the number of addresses present on the same subnet which have been identified as malicious.
6 blacklist_observations	Field providing the number of observations (of this IP) in the last 90 days.

Musubu API is available as a robust, yet easy-to-use RESTful web service for integrating into your in-house or 3rd party applications such as a SIEM

Through the Musubu API, users can query by a single IP Address or in bulk with simple parameters, including (1) the IPv4 address to investigate, (2) the API key string, (3) format (test or JSON), and (4) level (terse or verbose).

We also provide a clean user interface for daily use with one or up to 50 IPs available right on our site at https://app.musubu.io, as well as simple clients libraries in Python, Java, Perl, and others upon request. As well, Musubu can be integrated easily with most major SIEM tools such as IBM QRadar and Splunk. You can obtain the code and more at https://musubu.io/developers/.

Built-in security data complement other tool outputs to complete your cyber threat picture.

Secure B2B and consumer APIs.

Companies with public APIs can measure and monitor API connection activity. Companies can also use this mechanism to inform client callers of potential threats, better securing both organizations.

APIs are an underestimated source of vulnerabilities that scanners can easily miss. Even resource-rich organizations like T-Mobile and Salesforce have fallen prey to attacks leveraging API vulnerabilities.[iv] [v]

By checking the cybersecurity status of client API calls to determine if source calls are a cyber risk to them, organizations can limit access to APIs from certain locations and reduce their risk.

Personalize and secure web or mobile apps.

By using geolocation information from the API, web developers and businesses can deliver localized content on their sites and market to specific audiences, so different users get tailored content. This facilitates location-based A/B testing of products and content and promotes hyper-local content and events.

Simultaneously, organizations can use Musubu to secure mobile apps and web browsing by preventing apps from contacting high-risk APIs and blocking potentially malicious file uploads originating from high-risk IP addresses. Organizations can control access by location or threat level. Similarly, users can utilize Musubu data to alert users to risky websites.

Integrate into your SIEM for enhanced cyber response.

Musubu can enhance users' ability to identify and monitor network security events. By pulling data into the SIEM for external IPs and/or IP's hitting your network, organizations can better prioritize higher threat-scored IPs to investigation.

In fact, by aggregating enriched, network-centric data about activity and potential threats, the tool can:

(1) instantly alert security personnel to malicious activity,
(2) reduce response time to cyber threats across networks, *and*
(3) allow analysts to focus on faster containment and remediation.

Even absent specific security events, Musubu enables organizations to build a single operational picture across the enterprise.

Improve firewall performance.

Most commonly-used firewall solutions allow pluggable data sets and sources for network administrators to enhance or add whitelist and blacklist rule sets, to better recognize and stop malicious traffic.

With Musubu API, it's easy to plug our cyber threat data, score, and threat type by IP Address into your firewall, so you can better exclude potentially harmful types of traffic. We tag IPs with observed cyber threat types such as Botnets, Phishing, and Ransomware. Admins can then create any rules they wish to blacklist types of threats, geographic sources, or threat scores. This makes it easy to make your enterprise safer by controlling access to valuable websites, APIs, and other network endpoints.

Musubu applies the power of Big Data and Machine Learning to cyber and threat data.

Conclusion

Musubu takes a network-focused approach to understanding the IP addresses interacting with your organization. It incorporates information about the types of activities and entire network engages in, as well as geographical data that can pinpoint activity originating in regions known to be supportive of criminal activity. Integrating Musubu into your organization's existing security infrastructure makes this enriched data available at a click.

And by assessing the activity at the network level, rather than at the IP address, organizations can better contextualize, identify, and act upon the insight. Whether that means serving *legitimate* sales customers content that is more likely to convert, or better securing the APIs upon which your organization's operations rely, the result is better business and a safer internal network.

If you're operating without the benefit of these powerful filtering approaches, contact us at sales@musubu.io. Our experienced team will explain how Musubu can give you the edge in business and in cyber defense.

Musubu

About

Cyber security is people + technology.

Musubu provides your organization with fully-integrated, flexible cyber analysis services within your environment built on decades of experience and using superior analytics solutions to meet your cyber threats for today and tomorrow.

In additional to Musubu, our "Musubu Labs" works hard to provide innovative data streams and products that help you.

- ☑ Known Networks
- ☑ JediBadger
- ☑ Shadow Warrior
- ☑ PhishFry

Contact

Phone
(833) MUSUBU1
(833) 687-8281

Email
sales@musubu.io

Web
www.musubu.io

The information contained in this paper is for generalized informational and educational purposes only. It is not designed to substitute for, or replace, professional business advice. You must not rely on the information in the report as an alternative to professional business advice from an appropriately qualified professional. If you have any specific questions about any relevant subject matter, you should consult an appropriately qualified professional. **Release 2 Innovations, Inc.** does not represent, warrant, undertake or guarantee that the use of guidance in the report will lead to any particular outcome or result. The views and opinions expressed in this paper represent the opinion of the author(s) and do not necessarily represent the views or opinions of **Release 2 Innovations, Inc.**

Copyright © 2018 Release 2 Innovations, Inc. All rights reserved.

References

[i] https://www.cisco.com/c/dam/m/sl_si/events/2017/cisco-connect/pdf/ConnectSLO_What-can-you-lose_Security_2015-03-16-v3.pdf
[ii] https://www.csoonline.com/article/3191379/data-protection/false-positives-still-cause-alert-fatigue.html
[iii] http://www.ponemon.org/blog/new-ponemon-study-on-malware-detection-prevention-released
[iv] https://searchcloudsecurity.techtarget.com/tip/How-to-monitor-and-detect-a-cloud-API-vulnerability
[v] https://www.whitehatsec.com/blog/api-vulnerabilities/