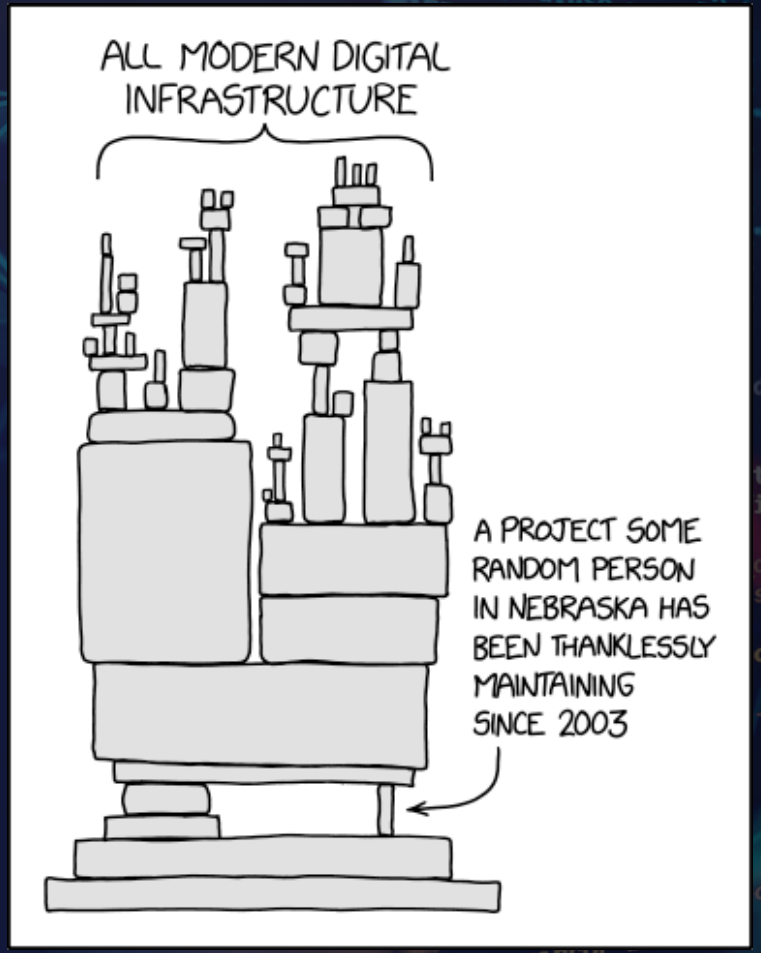

DARK SKY
TECHNOLOGY
Finally. Trust in Open Source
WWW.DARKSKYTECHNOLOGY.COM

Intentional Supply Chain Exploit

- Two researchers from the University of Minnesota.
- Intentionally submitted malicious code into Linux Kernel.
- Permanently banned from future submissions.

Trust is difficult to gain, even harder to prove, and easy to destroy in an instant…



https://xkcd.com/2347/

98% of code bases, even proprietary, now contain open-source software.

73% of code bases have at least one license issue.

67% of code bases contain at least one license conflict.

The average code base contains 445 open-source components.

How ‘bout security?

What (and who) is in our software?

How many other malicious contributions have been injected into the packages we're pulling into our systems and applications? What code is in our systems? And, who developed it?

75% of code bases contain FOSS with unpatched vulnerabilities

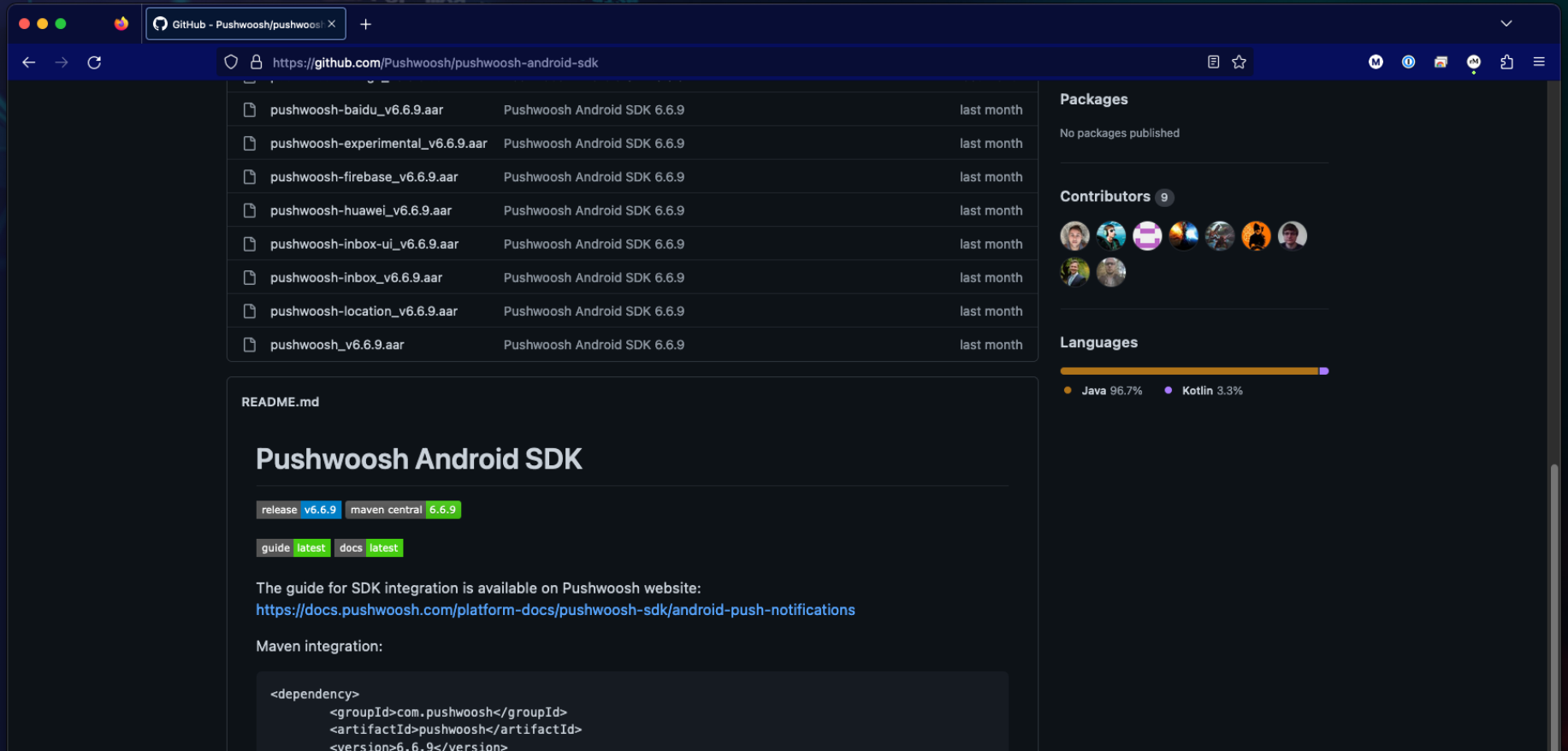
49% of code bases with open-source contain high-risk vulnerabilities.

82% of code bases contain open-source components that are at least four years out of date.

43% contain 10+ year old vulnerabilities.

2019 Open Source Risk and Security Analysis (OSSRA) report

Pushwoosh


GitHub - Pushwoosh/pushwoosh
https://github.com/Pushwoosh/pushwoosh-android-sdk
pushwoosh-baidu_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-experimental_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-firebase_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-huawei_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-inbox-ui_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-inbox_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh-location_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
pushwoosh_v6.6.9.aar Pushwoosh Android SDK 6.6.9 last month
Packages
No packages published
Contributors 9
Languages
Java 96.7%
Kotlin 3.3%
README.md
Pushwoosh Android SDK
release v6.6.9
maven central 6.6.9
guide latest
docs latest
The guide for SDK integration is available on Pushwoosh website:
https://docs.pushwoosh.com/platform-docs/pushwoosh-sdk/android-push-notifications
Maven integration:
<dependency>
<groupId>com.pushwoosh</groupId>
<artifactId>pushwoosh</artifactId>
<version>6.6.9</version>

NOT an American Company

The Story…

https://www.facebook.com › ... › Pushwoosh

Pushwoosh | Kensington MD - Facebook

Pushwoosh, **Kensington**, Maryland. 738 likes · 3 talking about this. The top mobile-inspired customer engagement platform trusted by 80000 clients from...

https://www.linkedin.com › company › pushwoosh

Pushwoosh - LinkedIn

Pushwoosh. IT Services and IT Consulting. **Kensington**, Maryland 978 followers. Mobile-inspired customer engagement platform for high achievers.

https://eintaxid.com › company › 352507621-pushwoo...

EIN 35-2507621 - Pushwoosh Inc., Kensington, Maryland

Pushwoosh Inc. is a small employer located at **Kensington**, Maryland. The employer identification number (EIN) for **Pushwoosh** Inc. is 352507621.

Our Exposure…

9 minute read · November 16, 2022 10:28 AM MST · Last Updated 2 months ago

EXCLUSIVE Russian software disguised as American finds its way into U.S. Army, CDC apps

U.S. Govt. Apps Bundled Russian Code With Ties to Mobile Malware Developer

November 28, 2022

Home › News › Security

Russian Code Found in US Army, CDC Apps

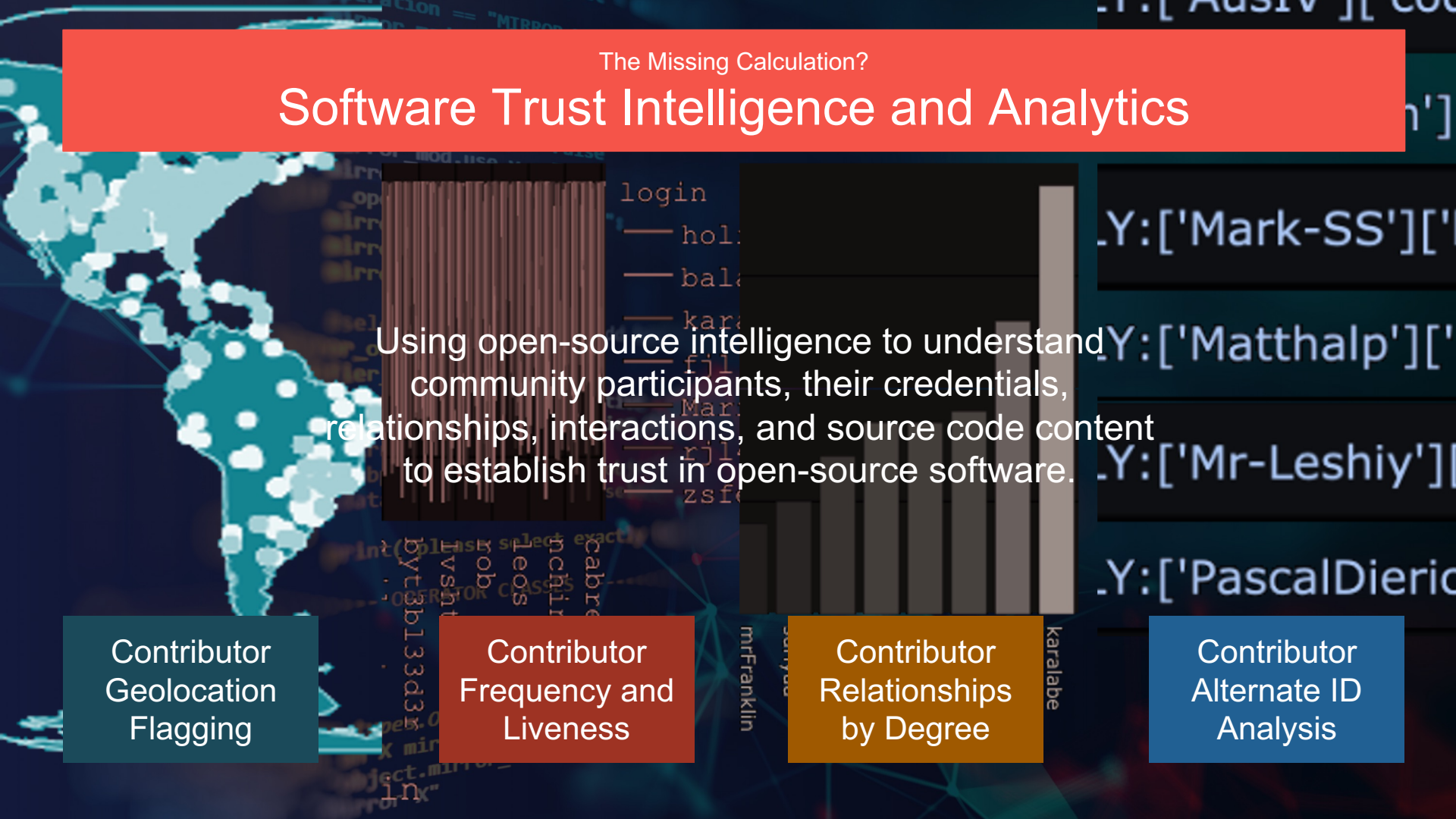
Everyone thought Pushwoosh was a US company, not a Russian entity operated from Siberia with its code embedded in 8,000 mobile apps.

By Matthew Humphries

November 14, 2022

The Missing Calculation?

Software Trust Intelligence and Analytics



Using open-source intelligence to understand community participants, their credentials, relationships, interactions, and source code content to establish trust in open-source software.

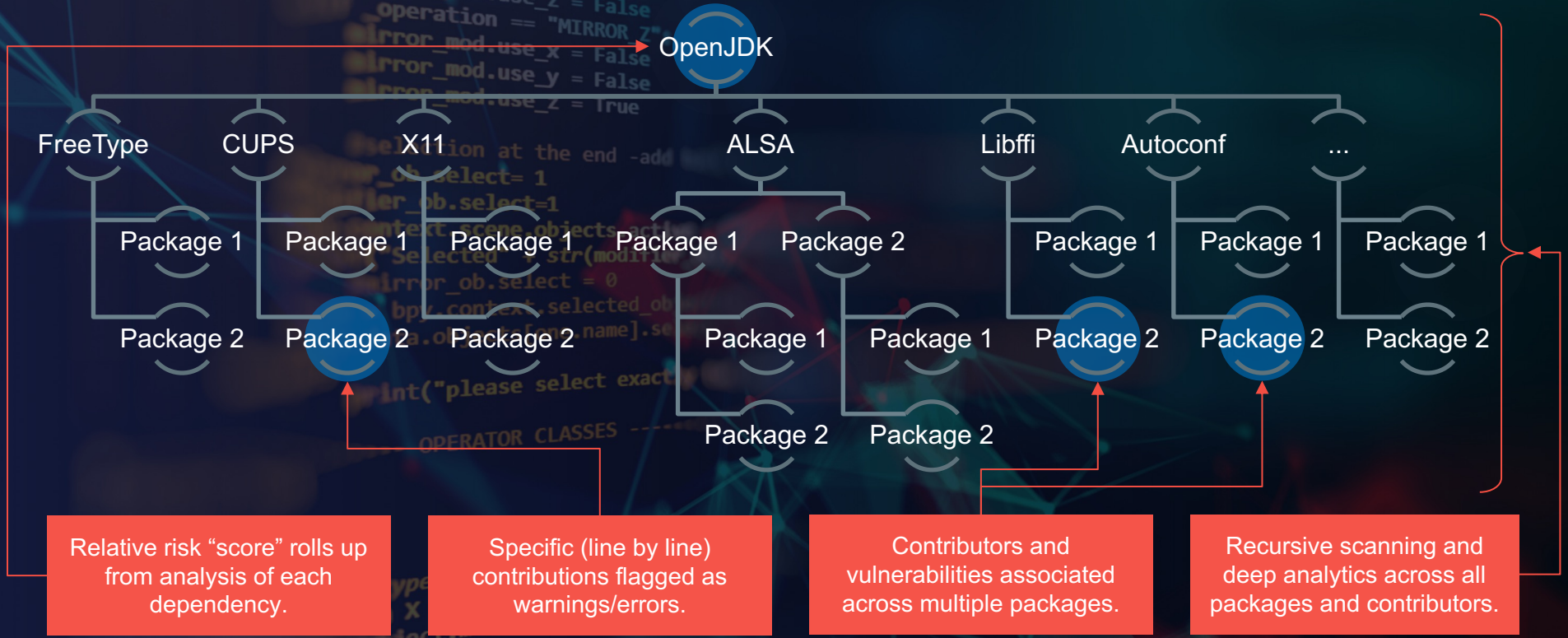
Contributor Geolocation Flagging

Contributor Frequency and Liveness

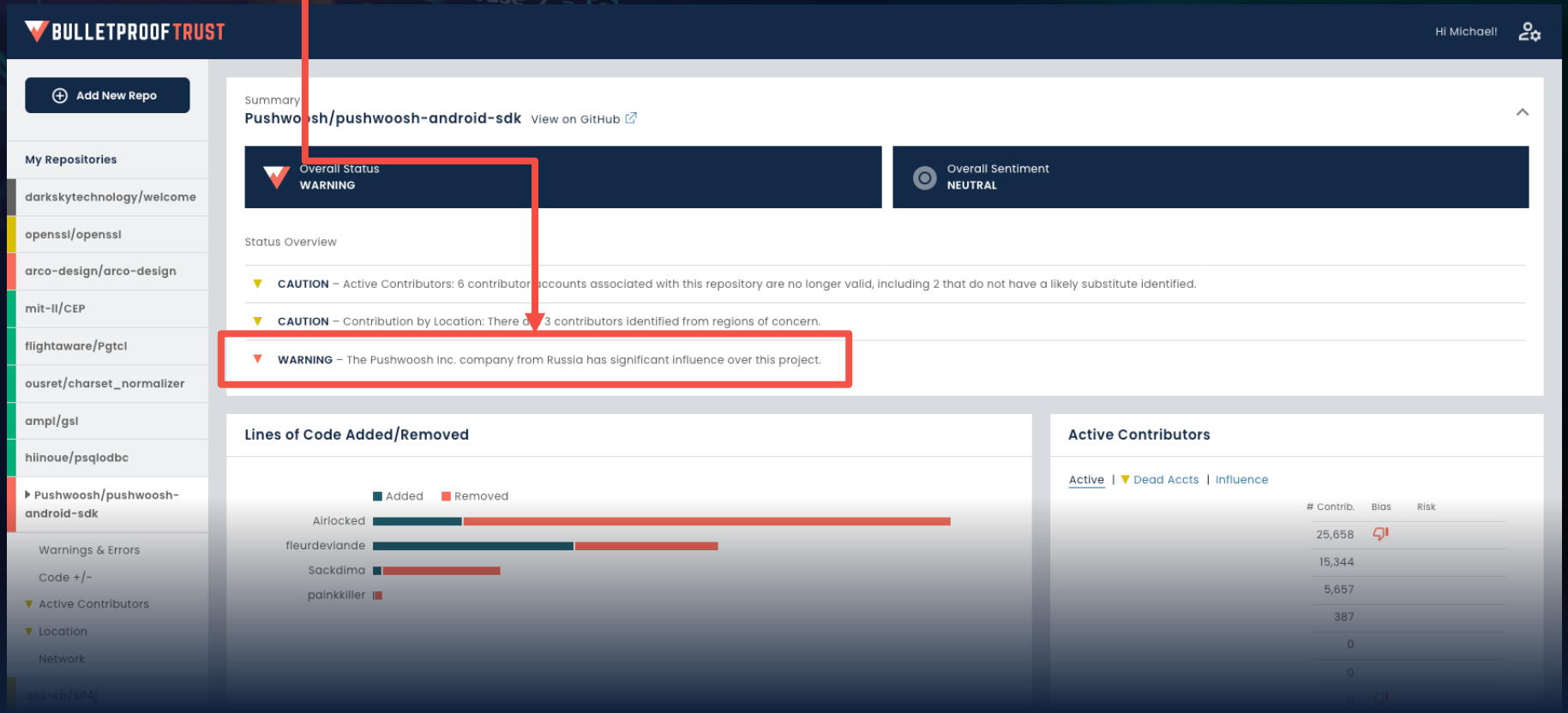
Contributor Relationships by Degree

Contributor Alternate ID Analysis

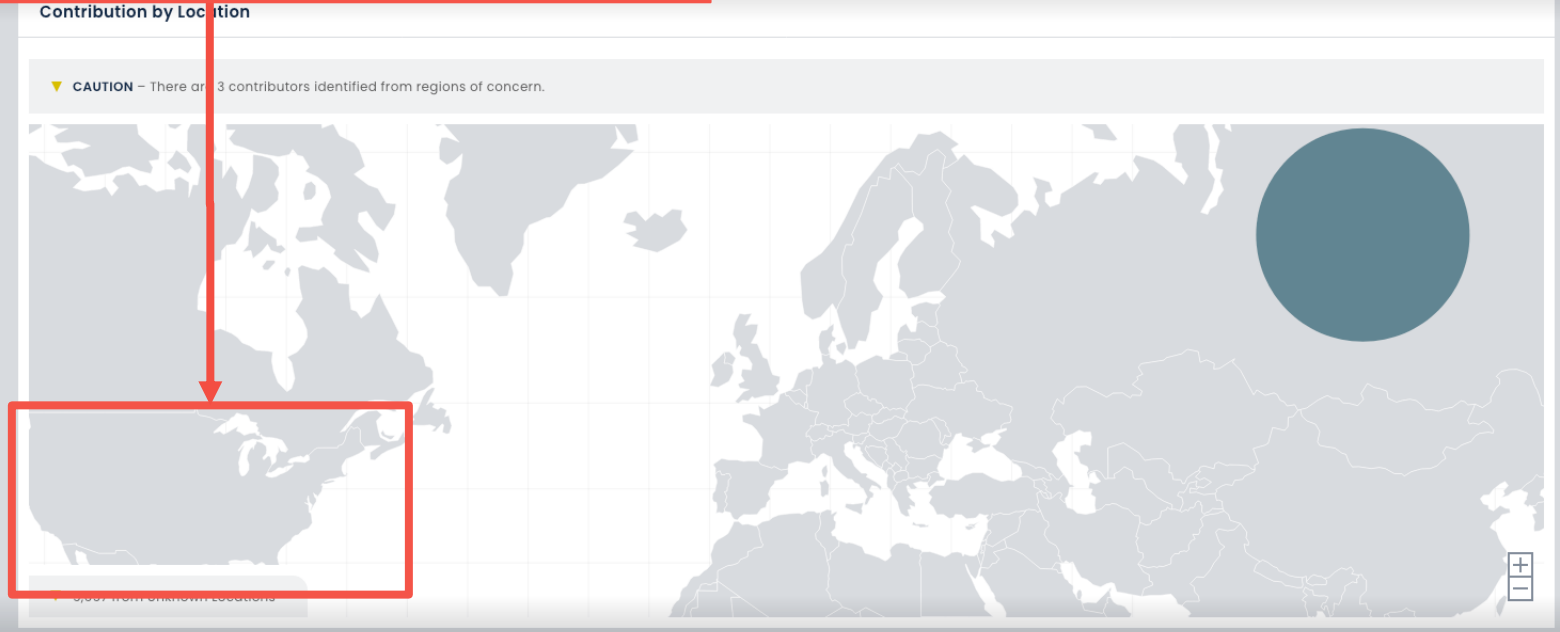
Identifying and Aggregating Layers of Risk



Back to Pushwoosh…



No Contributions in America



Contributor Network | Country | Company | Status | Reset

Thousands in Russia

qos-ch/slf4j@v_1.7.30

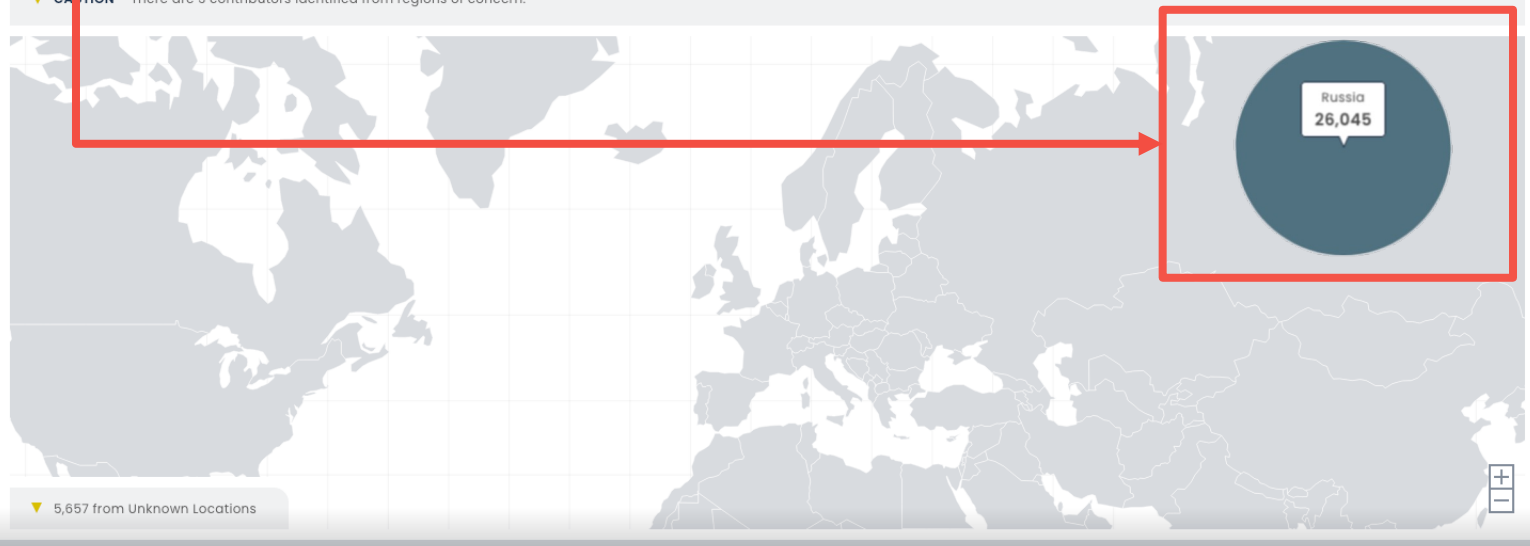
OpenXT/meta-selinux

12K 14K 16K 18K 20K 22K 24K 26K

0 0 0 0 0

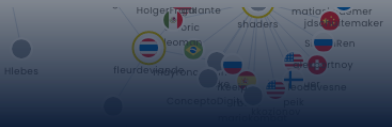
Contribution by Location

CAUTION – There are 3 contributors identified from regions of concern.

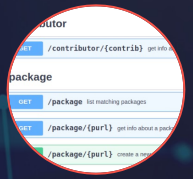


5,657 from Unknown Locations

Contributor Network Country Company Status Reset

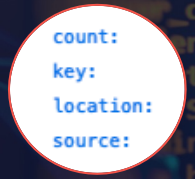


With Russian and Hidden Influencers



Collection and Analysis

Preserve Historical Contributions

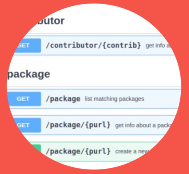


Enhanced Contributor Data

Open Source Package Intelligence

Enhanced Data Security & Control

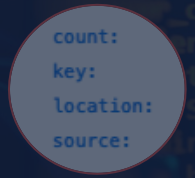
OSINT + Analysis



Collection and Analysis

A method for asynchronously collecting and analyzing OSINT from hundreds (or thousands) of sources

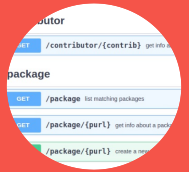
Preserve Historical Contributions



Enhanced Contributor Data

Open Source Package Intelligence

Enhanced Data Security & Control



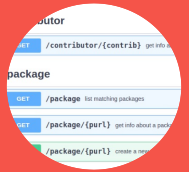
Collection and Analysis

A method for asynchronously collecting and analyzing OSINT from hundreds (or thousands) of sources

Collectors

Analysis Engines

Services that automatically scale up and down in clusters based on load.



Collection and Analysis

A method for asynchronously collecting and analyzing OSINT from hundreds (or thousands) of sources

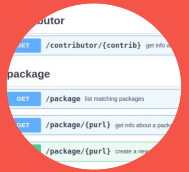
Collectors

LinkedIn
Reddit
Hacker.net
Etc…

Analysis Engines

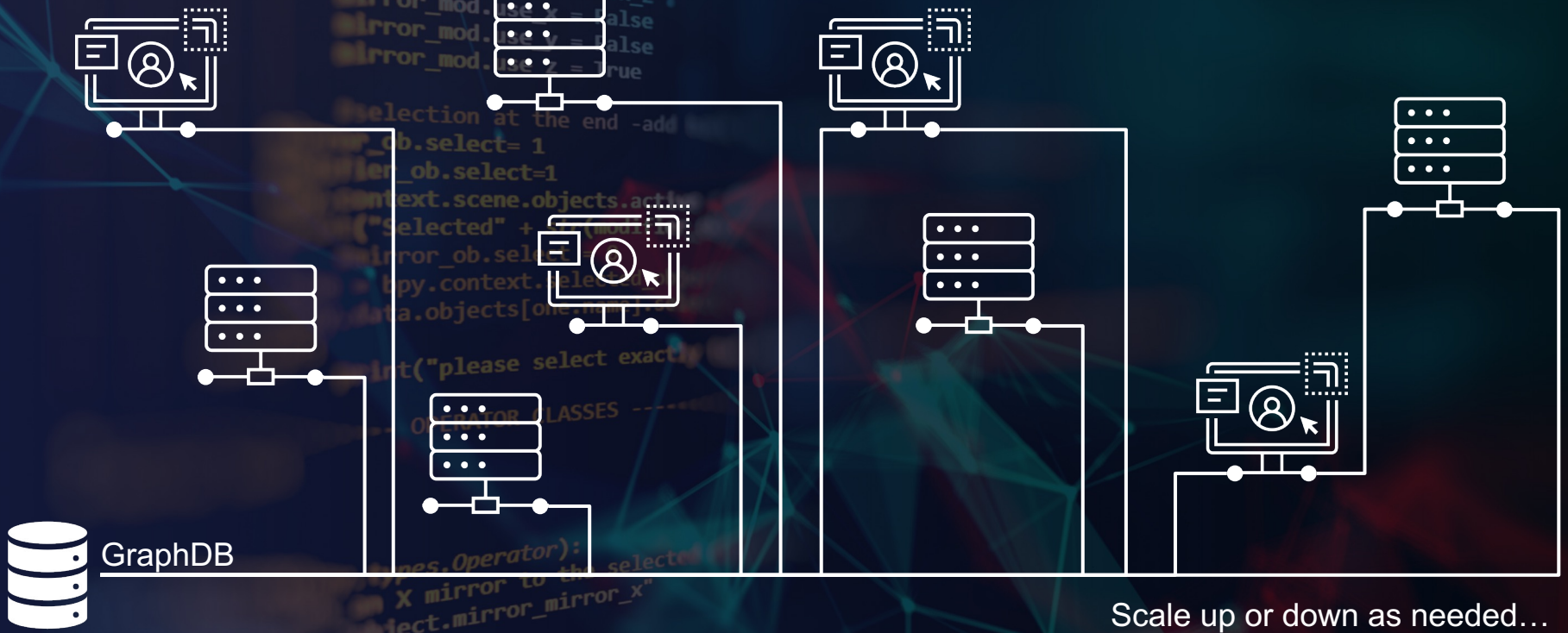
Geo Analysis
Nationality Check
Work/Skills History
Etc.

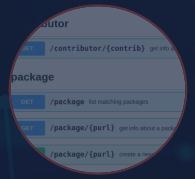
GraphDB



Collection and Analysis

A method for asynchronously collecting and analyzing OSINT from hundreds (or thousands) of sources

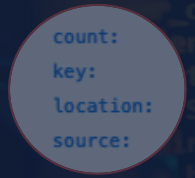




Collection and Analysis

Preserve Historical Contributions

Pulling history from pre-GitHub packages (i.e., capture and merge contributors from Source Forge)



Enhanced Contributor Data

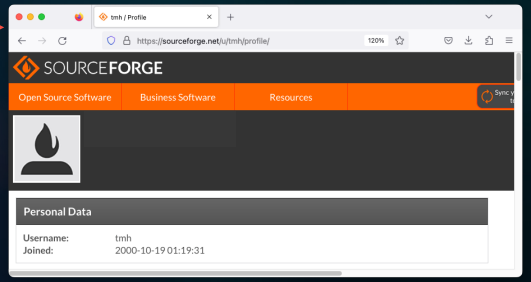
Open Source Package Intelligence

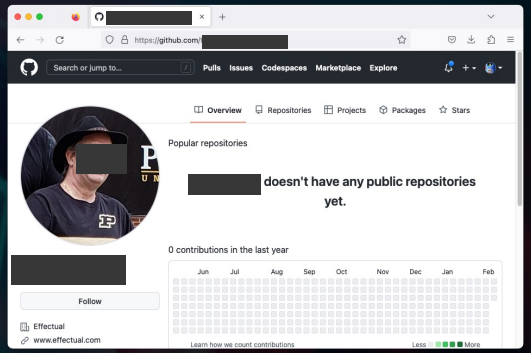
Data Security and Control

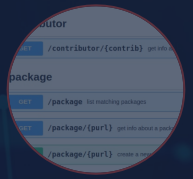
Preserve Historical Contributions

Pulling history from pre-GitHub packages (i.e., capture and merge contributors from Source Forge)

```
server — -zsh — 138×53
(.venv) coder@Sandys-MBP server % python scripts/manual_svn_link.py -n sm-shaw-Oratcl -s  https://svn.code.sf.net/p/oratcl/svncode/
Adding https://svn.code.sf.net/p/oratcl/svncode/ to the sm-shaw-Oratcl package
Appending the following authors:
UserID: [tmh]
Lines Changed: [1360]
Commit Timezone: -0700,-0600
First Commit: [2000-05-24]
Last Commit: [2017-11-23]


UserID: [hobbs]
Lines Changed: [30]
Commit Timezone: -0700
First Commit: [2004-11-22]
Last Commit: [2006-01-25]


UserID: [bhlewis]
Lines Changed: [24]
Commit Timezone: -0600,-0700
First Commit: [2000-11-08]
Last Commit: [2001-07-24]


UserID: [mtariq]
Lines Changed: [162]
Commit Timezone: -0600,-0700
First Commit: [1999-07-26]
Last Commit: [2000-09-14]


UserID: [wart]
Lines Changed: [74]
Commit Timezone: -0600,-0700
First Commit: [1999-09-16]
Last Commit: [2000-09-07]


UserID: [davidg]
Lines Changed: [2]
Commit Timezone: -0600
First Commit: [2000-07-19]
Last Commit: [2000-07-19]


UserID: [surles]
Lines Changed: [2]
Commit Timezone: -0600
First Commit: [1999-09-21]
Last Commit: [1999-09-21]


(.venv) coder@Sandys-MBP server %
```

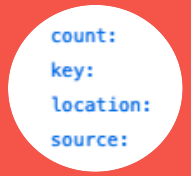






Collection and Analysis

Preserve Historical Contributions



Enhanced Contributor Data

Contributor commit date range, signing details, repo popularity, activity, etc.

Open Source Package Intelligence

Data Security and Control

count:
key:
location:
source:

Enhanced Contributor Data

Contributor commit date range, signing details, repo popularity, activity, etc.

Summary

ampl/gsl@v2.5.0 View on GitHub

Overall Status
GOOD

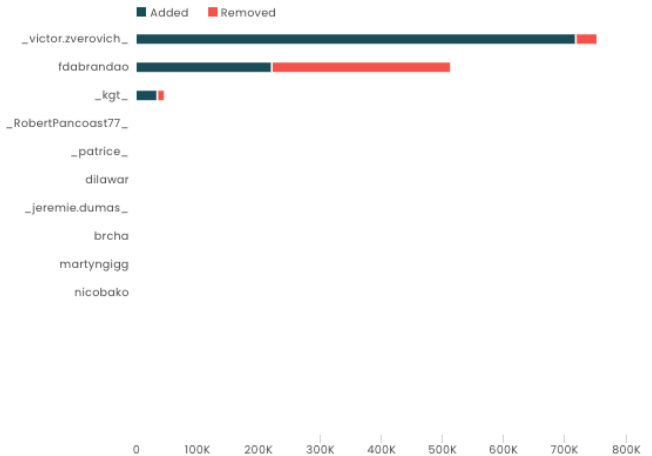
Overall Sentiment
NEUTRAL

Software Bill of Materials (SBOM)

<?xml version="1.0" encoding="UTF-8"?><bom serialNumber="urn:uuid:bcb6253e-2e18-45c0-873f-f3e2d8ccc3d3" version="1" xmlns="http://cyclonedx.org/schema/bom/1.4"><metadata><timestamp>2023-02-01T14:52:21.016727+00:00</timestamp><tools><tool><vendor>CycloneDX</vendor><name>cyclonedx-bom</name><version>3.10.1</version></tool><tool><vendor>CycloneDX</vendor><name>cyclonedx-python-lib</name><version>3.1.5</version><externalReferences><reference type="build-system"><url>https://github.com/CycloneDX/cyclonedx-python-lib/actions</url></reference><reference type="distribution"><url>https://pypi.org/project/cyclonedx-python-lib/</url></reference><reference type="documentation"><url>https://cyclonedx.github.io/cyclonedx-python-lib/</url></reference><reference type="issue-tracker"><url>https://github.com/CycloneDX/cyclonedx-python-lib/issues</url></reference><reference type="license"><url>https://github.com/CycloneDX/cyclonedx-python-lib/blob/main/LICENSE</url></reference><reference type="release-notes"><url>https://github.com/CycloneDX/cyclonedx-python-lib/blob/main/CHANGELOG.md</url></reference><reference type="vcs"><url>https://github.com/CycloneDX/cyclonedx-python-lib</url></reference><reference type="website"><url>https://cyclonedx.org/</url></reference></externalReferences></tool></tools></metadata><components><component bom-ref="2b58d5b1-dc5b-4cd8-ad64-7df63f4ed5be" type="library"><author>Kenneth Reitz</author><name>certifi</name><version>2022.12.7</version><licenses><license><name>MPL-2.0</name></license><license><name>Mozilla Public License 2.0 (MPL 2.0)</name></license></licenses><purl>pkg:pypi/certifi@2022.12.7</purl></component><component bom-ref="9b07d9cc-05a9-4091-8efb-fc92fa253ef4" type="library"><author>Ahmed TAHRI @Ousret</author><name>charset-normalizer</name>

Download SPDX | Download Cyclone DX

Lines of Code Added/Removed



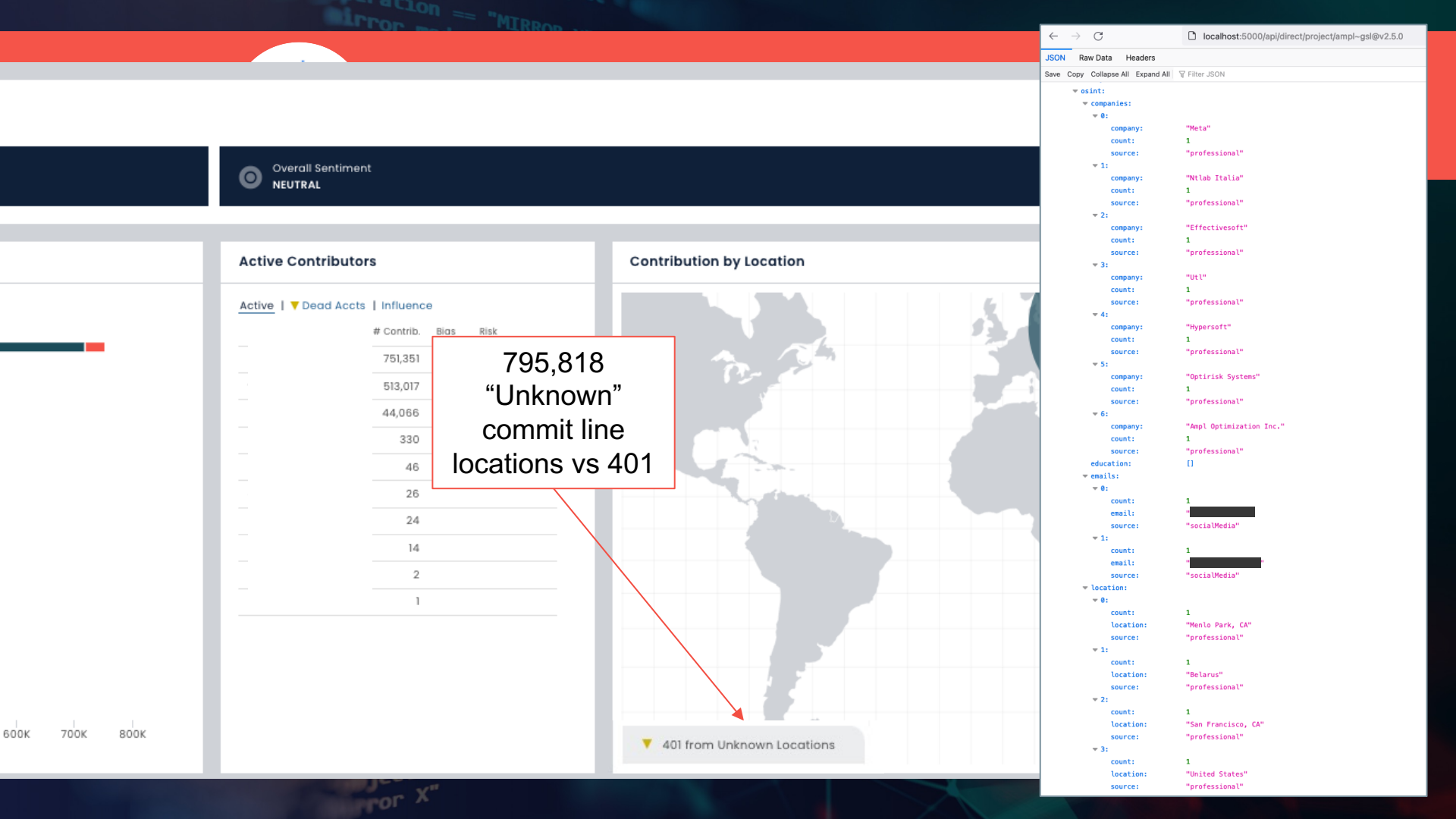
Active Contributors

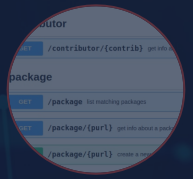
Active | Dead Accts | Influence

	# Contrib.	Bias	Risk
	751,351		
	513,017		
	44,066		
	330		
	46		
	26		
	24		
	14		
	2		
	1		

Contribution by Loc

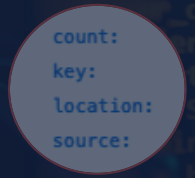
795,818 from Unkno


Overall Sentiment
NEUTRAL
Active Contributors
Active | Dead Accts | Influence
Contrib. Bias Risk
751,351
513,017
44,066
330
46
26
24
14
2
1
795,818 “Unknown” commit line locations vs 401
Contribution by Location
401 from Unknown Locations
600K
700K
800K
localhost:5000/api/direct/project/ampl~gsl@v2.5.0
JSON Raw Data Headers
Save Copy Collapse All Expand All Filter JSON
osint:
companies:
0:
company: "Meta"
count: 1
source: "professional"
1:
company: "Ntlab Italia"
count: 1
source: "professional"
2:
company: "Effectivesoft"
count: 1
source: "professional"
3:
company: "Util"
count: 1
source: "professional"
4:
company: "Hypersoft"
count: 1
source: "professional"
5:
company: "Optirisk Systems"
count: 1
source: "professional"
6:
company: "Ampl Optimization Inc."
count: 1
source: "professional"
education: []
emails:
0:
count: 1
email: "[redacted]"
source: "socialMedia"
1:
count: 1
email: "[redacted]"
source: "socialMedia"
location:
0:
count: 1
location: "Menlo Park, CA"
source: "professional"
1:
count: 1
location: "Belarus"
source: "professional"
2:
count: 1
location: "San Francisco, CA"
source: "professional"
3:
count: 1
location: "United States"
source: "professional"



Collection and Analysis

Preserve Historical Contributions



Enhanced Contributor Data

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

Data Security and Control

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

Save Copy Collapse All Expand All Filter JSON

```
▼ repoActivity:
  ▼ issues:
      closedAverageDaysOpen:    191.6
      closedCount:              35
      closedLongestDaysOpen:    1466
      closedModeDaysOpen:       0
      closedShortestDaysOpen:   0
      openAverageDaysOpen:      656.71
      openCount:                7
      openLongestDaysOpen:      1990
      openModeDaysOpen:         1990
      openShortestDaysOpen:     47
  ▼ license:
      description:              "GNU General Public License v3.0"
      name:                     "gpl-3.0"
```

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

```
openLongestDaysOpen:        1990
description:                "GNU General Public License v3.0"
name:                       "gpl-3.0"
spdxId:                     "GPL-3.0"
▼ origination:
isFork:                     false
origin:                     null
▼ popularity:
downloads:                  true
forks:                      182
stars:                      445
watchers:                   43
primaryLanguage:            "C"
▼ pullRequests:
closedAverageDaysOpen:      15.21
closedCountMerged:          24
closedCountUnmerged:        0
```

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

```
    watchers:                43
  primaryLanguage:           "C"
▼ pullRequests:
    closedAverageDaysOpen:   15.21
    closedCountMerged:       24
    closedCountUnmerged:     0
    closedLongestDaysOpen:   322
    closedModeDaysOpen:      0
    closedShortestDaysOpen:  0
    openAverageDaysOpen:     805.5
    openCount:               2
    openLongestDaysOpen:     1581
    openModeDaysOpen:        1581
    openShortestDaysOpen:    30
▼ versions:
    releaseCount:            1
```

Open Source Package Intelligence

Versioning, issues, popularity, timezones, and signing

JSON Raw Data Headers

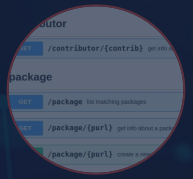
Save Copy Collapse All Expand All Filter JSON


```
▼ 0:
    timeZone:          "-0600"
    timeZoneCount:     3
▼ 1:
    timeZone:          "-0500"
    timeZoneCount:     2
▼ 2:
    timeZone:          "+0000"
    timeZoneCount:     42
  firstCommit:         "2016-06-14 06:25:12 +0000"
  lastCommit:          "2022-02-08 18:13:29 -0600"
  linesAdded:          5128
  linesRemoved:        0
  mergeCommitsCount:   0
▶ identification:      {…}
▶ location:            {…}
▶ osint:               {…}
```

Open Source Package Intelligence

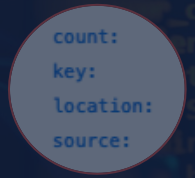
Versioning, issues, popularity, timezones, and signing

```
timeZoneCount:    3
timeZoneCount:    42
firstCommit:      "2016-06-14 06:25:12 +0000"
lastCommit:       "2022-02-08 18:13:29 -0600"
linesAdded:       5128
linesRemoved:     0
mergeCommitsCount: 0
▶ identification: {…}
▶ location:       {…}
▶ osint:          {…}
▼ security:
    signed:       0.09
```



Collection and Analysis

Preserve Historical Contributions



Enhanced Contributor Data

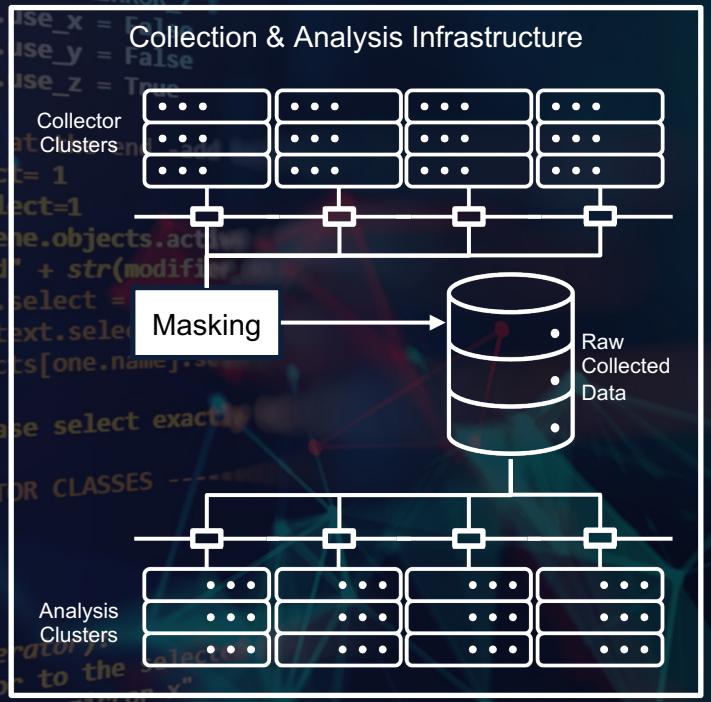
Open Source Package Intelligence

Data Security and Control

Properly handling and protecting personally identifiable information (PII)

Data Security and Control

Properly handling and protecting personally identifiable information (PII)



The Solution?

DARK SKY TECHNOLOGY

Build **software bill of materials (SBOM)** to identify all packages and dependencies	Identify ALL code found in the integrated package
Track **Trust Analytics** through all integrated packages and all dependencies	Helps identify weaknesses by valid contributors
Flag CVEs and other **code vulnerabilities** throughout entire dependency chain and associate their "blame" with contributor networks	Identify quality of development teams
Correlate **code contributions** with analytics of concern (geography, liveness, connectedness, code quality, past vulnerabilities, outside influences, etc)	Flags potential contribution issues beyond CVEs
Automate inspection of flagged and concerning code based on Trust Analytics (and eventually... automate **resolution** though code transformation)	Specify and resolve current and future code issues

Preventing Supply Chain Exploits

- Analytics can help flag unusual check-ins for analysis.
- Unusual developer activity can trigger deeper analysis.
- Once caught, bad actors will forever be flagged.
- All future code will be labeled as suspect until trust is reestablished.

Bad actors cannot hide (for long)…
Their “signatures” will trigger warnings and errors, preventing intentionally or accidentally submitted code vulnerabilities and eventual system exploit.

DARK SKY
TECHNOLOGY

Finally. *Trust* in Open Source

INFO@DARKSKYTECHNOLOGY.COM