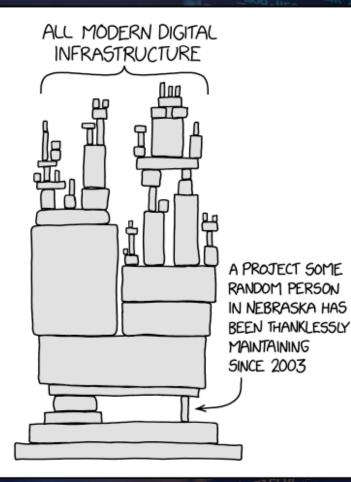




### **Intentional Supply Chain Exploit**

- 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...



98% of code bases, even proprietary, now contain opensource software.

How 'bout security?

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 opensource components.

### 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contain high-risk vulnerabilities. 82% of code bases contain opensource components that are at least four years out of date.

43% contain 10+ year old vulnerabilities.

https://xkcd.com/2347/

2019 Open Source Risk and Security Analysis (OSSRA) report

# Pushwoosh

•••	GitHub - P	Pushwoosh/pushwoosh× +				~
$\leftarrow \  \  \rightarrow \  \   G$		https://github.com/Pushwa	oosh/pushwoosh-android-sdk		□ ☆	0 🖉 🤗 දා =
		🗋 pushwoosh-baidu_v6.6.9.	aar Pushwoosh Android SDK 6.6.9	last month	Packages	
		D pushwoosh-experimental	v6.6.9.aar Pushwoosh Android SDK 6.6.9	last month	No packages published	
		pushwoosh-firebase_v6.6	.9.aar Pushwoosh Android SDK 6.6.9	last month	O antributant C	
		pushwoosh-huawei_v6.6.9	9.aar Pushwoosh Android SDK 6.6.9	last month	Contributors 9	
		pushwoosh-inbox-ui_v6.6	.9.aar Pushwoosh Android SDK 6.6.9	last month	🔞 🛞 🚍 👶 🌮 😩 🔕	
		🕒 pushwoosh-inbox_v6.6.9.4	aar Pushwoosh Android SDK 6.6.9	last month	(2)	
		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	Languages	
		README.md			<ul> <li>Java 96.7%</li> <li>Kotlin 3.3%</li> </ul>	
		Pushwoosh A	Android SDK			
		release v6.6.9 maven central	6.6.9			
		guide latest docs latest				
			ation is available on Pushwoosh website: com/platform-docs/pushwoosh-sdk/android-pus	sh-notifications		I
		Maven integration:				
			pushwoosh ushwoosh			

<version>6.6.9</version>

### irror mod.use x The Story... Our Exposure... 9 minute read · November 16, 2022 10:28 AM MST · Last Updated 2 months Home > News > Security https://www.facebook.com > ... > Pushwoosh ago Pushwoosh | Kensington MD - Facebook Russian Code Found in US Army, **EXCLUSIVE Russian software disguised as** Pushwoosh, Kensington, Maryland. 738 likes · 3 talking about this. The top mobile-inspired American finds its way into U.S. Army, CDC customer engagement platform trusted by 80000 clients from ... **CDC** Apps apps https://www.linkedin.com > company > pushwoosh Pushwoosh - LinkedIn

U.S. Govt. Apps Bundled

**Russian Code With Ties to** 

Pushwoosh. IT Services and IT Consulting. Kensington, Maryland 978 followers. Mobileinspired 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.

### embedded in 8,000 mobile apps. Mobile Malware Developer By Matthew Humphries November 14, 2022 November 28, 2022

Everyone thought Pushwoosh was a US company, not a

Russian entity operated from Siberia with its code

🗧 🔍 😫 💭 GitHub - Pu	ishwoosh/pushwoosh× +						$\sim$	
$\leftarrow \rightarrow G$	C A https://github.com/Pushwoosh/pushw	oosh-android-sdk		目 ☆	0 М	<b>a</b>	🔌 பி	≡
	pushwoosh-baidu_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month	Packages				
	pushwoosh-experimental_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month	No packages published				
	pushwoosh-firebase_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month	O and the state of the				
	🗋 pushwoosh-huawei_v6.6.9.aar	Pushwoosh Android SDK 6.6.9	last month	Contributors 9				
	🗋 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					
	nuchwooch v669 aar	Buchwooch Android SDK 669	last month	Languages				

## **NOT** an American Company

### 

## The Missing Calculation? Software Trust Intelligence and Analytics

login

-bala

mrFranklin



.Y:['Mark-SS']['

Using open-source intelligence to understandY:['Matthalp'][' community participants, their credentials, ationships, interactions, and source code content to establish trust in open-source software. Y:['Mr-Leshiy']

Contributor Geolocation Flagging

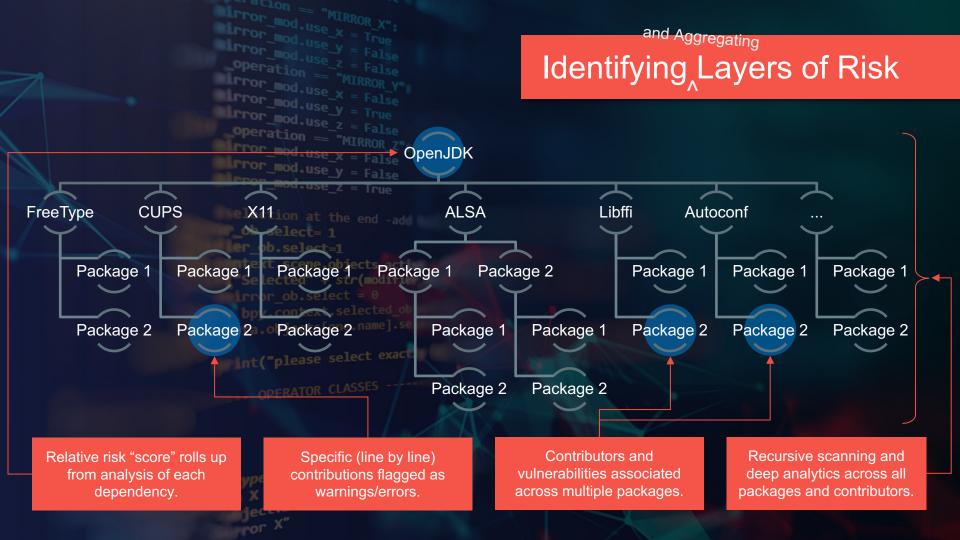


Contributor Relationships by Degree

caralabe

## .Y:['PascalDieric

Contributor Alternate ID Analysis



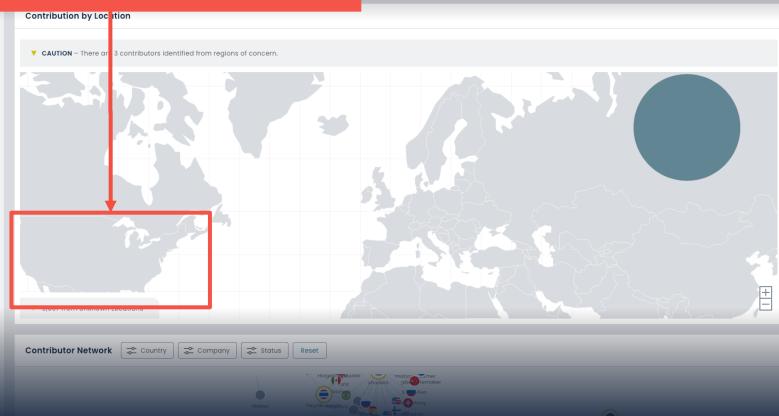
## Back to Pushwoosh...

<b>W</b> BULLETPROOF <b>TRUS</b> 1	S. Lilod. USe 7 _ F.		Hi Michael!	°4
🕀 Add New Repo	Summary Pushwo sh/pushwoosh-android-sdk View on GitHub ⊡			^
My Repositories	Overall Status Overall Sentimen	1		
darkskytechnology/welcome	WARNING OVERAL SPIRITHEN			
openssi/openssi	Status Overview			
arco-design/arco-design	CAUTION – Active Contributors: 6 contributor accounts associated with this repository are no longer valid, including 2 that do not have a	likely substitute identified.		
mit-II/CEP	CAUTION – Contribution by Location: There d 3 contributors identified from regions of concern.			
flightaware/Pgtcl	WARNING - The Pushwoosh Inc. company from Russia has significant influence over this project.			
ousret/charset_normalizer				
ampi/gsi	Lines of Code Added/Removed	Active Contributors		
hiinoue/psqlodbc				
▶ Pushwoosh/pushwoosh-	Added Removed	Active   Vead Accts   Influence	ontrib. Bias Risk	
android-sdk	Airlocked		,658 <b>[]</b>	
Warnings & Errors	fleurdeviande		j,344	
Code +/-	Sackdima 🔳		5,657	
Active Contributors	painkkiller 🔳		387	
▼ Location				
Network				

qos-ch/slf4j@v\_1.7.30

OpenXT/meta-selinux

## No Contributions in America



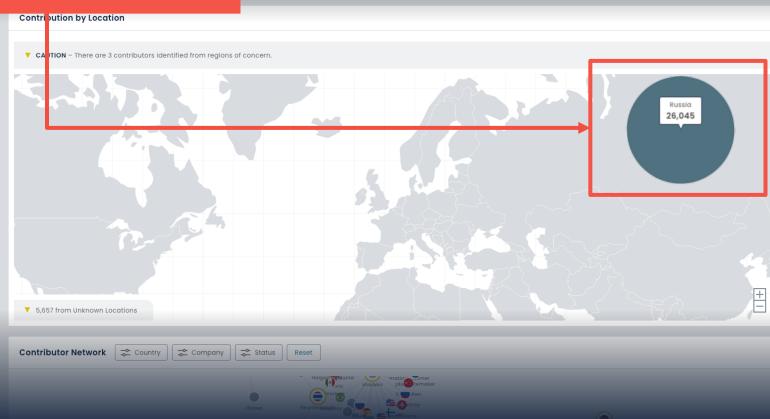
22K 24K 26K

0

qos-ch/slf4j@v\_1.7.30

OpenXT/meta-selinux

## Thousands in Russia



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

<u>ا</u>ل

0

## With Russian and Hidden Influencers

Contributor Network 🛛 😞	Country 🔁 Company 🔁 Statu	s Reset			
	•	fiel 10 10 10 10 10 10 10 10 10 10 10 10 10	tenar In Y		
			€ <b>С<sup>9</sup> ∦</b>		
		•		•	
				•	

© 2023 Dark Sky Technology. All rights reserved.





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

## Preserve Historical Contributions

count: key:

Enhanced Contributor Data

source:

**Open Source Package Intelligence** 

Enhanced Data Security & Control



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

Operation == "MIRROR\_Z"
Irror\_mod.use\_x = False
Irror\_mod.use\_y = False
Irror\_mod.use\_z = True

Collectors

vject.mirror\_mirror\_x

WOT X"

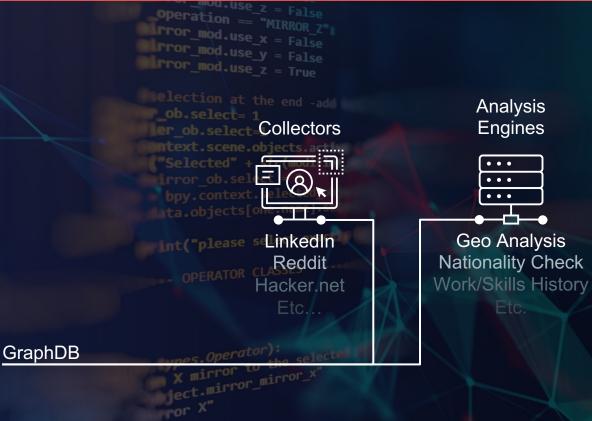




Services that automatically scale up and down in clusters based on load.

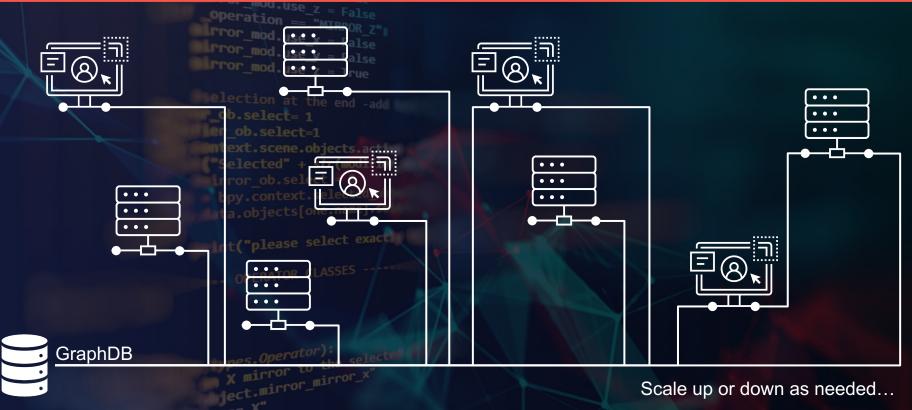


A method for asynchronously collecting and analyzing OSINT from hundreds (or thousands) of sources





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



### color contributor/(centrib) on more package or /package to maning package /package/(part) on show any of /package/(part) one contribution any of /package/(part) one contribution any of /package/(part) one contribution any of

key:

## **Collection and Analysis**

## **Preserve Historical Contributions**

**Enhanced Contributor Data** 

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

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)

<pre>vexpload/sdys/set server &amp; spload scripts/wexults/uncled = % Helps//wexult/incide/ infinits/incide/indice/ind</pre>		Openation Use_Z = False	
		server — -zsh — 138×53	
	dding https://svn.code.sf.net/p/oratcl/svnc ppending the following authors:		● ● ●  ●  ●  ●  ●  ●  ●  ●  ●  ●  ●  ●
surfice:       [Windows: 200]	ines Changed: [1360] commit Timezone: -0700,-0600 first Commit: [2000-05-24] ast Commit: [2017-11-23]	<pre>Pror_mod.use_z = True</pre>	SOURCE FORGE
<pre>verbs: [cont:: [c</pre>	iserID: [hobbs] ines Changed: [30] ommit Timezone: -0700 inst.commit: [2004-11-22] ast Commit: [2006-01-25]	<pre>ob.select=1</pre>	Open Source Software Business Software Resources Open Source Software Resources
<pre>lives.Compad: [120] mit Timescone: e000, e700 isst Commit: [1099-09-20] isst Commit: [1099-09-20] isst Commit: [1099-09-20] sat Commit: [1099-09-20]</pre>	iserID: [bhlewis] ines Changed: [24] commit Timezone: -0600,-0700 inst Commit: [2000-11-08] ast Commit: [2001-07-24]	<pre>Selected" + str(modifie rror ob.select = 0</pre>	Username: tmh
serDi: [vart] intes Changed: [7] and L' intescoil: - politici [1999-09-6]; ast Comit: [1999-09-6]; ast Comit: [1999-09-6]; intes Changed: [2] intes Changed: [2] inter Changed: [2]	<pre>serID: [mtariq] ines Changed: [162] ommit Timezone: -0600, -0700 irst Commit: [1999-07-26] ast Commit: [2000-09-14]</pre>	<pre>bpy.context.selected_cb data.objects[one.name].selected_cb</pre>	
serU: [dovidg] ines Changed: [2] omit T Inezone: -0600 irst Commit: [2900-07-19] serU: [2] ines Changed: [2] ines Changed	SerID: [wart] ines Changed: [74] cmmt Timezone: -0600,-0700 irst Commit: [1999-09-16] ast Commit: [2000-09-07]	operator classes	<ul> <li>← → C</li> <li>○ A https://github.com/</li> <li>○ A https://github.com/</li> <li>○ Barch or j.kmp to</li> <li>○ Barch or j.kmp to</li></ul>
Ines Changed: [2] ines Changed: [2] inst Commit: [1999-69-21] ast Commit: [1999-69-21] ist C	iserID: [davidg] ines Changed: [2] ommit Timezone: -0600 inst Commit: [2000-07-19] ast Commit: [2000-07-19]	UP LIVIN	Popular repositories
verv) coder@Sandye-MBP server \$	SerID: [surles] ines Changed: [2] ommit Timescone: -0600 inst Commit: [1999-09-21] ast Commit: [1999-09-21]	ypes.Operator): X mirror to the selecter	Follow     Image: Sep Oct. New Dice Jan Feb       Follow     Image: Sep Oct. New Dice Jan Feb
	.venv) coder@Sandys-MBP server %	lect. minu-	



## Preserve Historical Contributions

count: key: location: source:

## Enhanced Contributor Data

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

Open Source Package Intelligence

Data Security and Control

### count: kev: location: source:

## **Enhanced Contributor Data**

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

795,818 from Unkno

### u. Use z = Falso

### Summarv ampl/gsl@v2.5.0 View on GitHub 17 Overall Status **Overall Sentiment** GOOD NEUTRAL Software Bill of Materials (SBOM) Lines of Code Added/Removed Active Contributors Contribution by Lo <?xml version="1.0" encoding="UTF-8"?><born Active | V Dead Accts | Influence serialNumber="urn:uuid:bcb6253e-2e18-45c0-873f-f3e2d8ccc3d3" Added Removed version="1" xmIns="http://cyclonedx.org/schema/bom/1.4"><metadata> # Contrib Bigs Risk <timestamp>2023-02-01T14:52:21.016727+00:00</timestamp><tools><tool> \_victor.zverovich\_ 751,351 🖓 <vendor>CycloneDX</vendor><name>cyclonedx-bom</name> <version>3.10.1</version></tool><vendor>CycloneDX</vendor> fdabrandao 513.017 <name>cyclonedx-python-lib</name><version>3.1.5</version> \_kgt\_ <externalReferences><reference type="build-system"> 44,066 <url>https://github.com/CycloneDX/cyclonedx-python-lib/gctions</url> \_RobertPancoast77\_ </reference><reference type="distribution"><url>https://pypi.org/project 330 /cyclonedx-python-lib/</url></reference><reference \_patrice\_ type="documentation"><url>https://cyclonedx.github.io/cyclonedx-python-46 lib/</url></reference><reference type="issue-tracker"> dilawar <url>https://aithub.com/CvcloneDX/cvclonedx-pvthon-lib/issues</url> 26 </reference><reference type="license"><url>https://github.com/CycloneDX \_ieremie.dumas\_ /cyclonedx-python-lib/blob/main/LICENSE</url></reference><reference 24 type="release-notes"><url>https://github.com/CycloneDX/cyclonedxbrcha python-lib/blob/main/CHANGELOG.md</url></reference><reference 14 type="ycs"><url>https://aithub.com/CycloneDX/cyclonedx-python-lib</url> martyngigg </reference><reference type="website"><url>https://cyclonedx.org</url> 2 </reference></externalReferences></tool></tools></metadata> nicobako 1 <components><component bom-ref="2b58d5b1-dc5b-4cd8ad64-7df63f4ed5be" 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> 200K 500K 600K 800K Download Cyclone DX

### $\leftarrow \rightarrow C$ localhost:5000/api/direct/project/ampl~gsl@v2.5.0 JSON Raw Data Headers Save Copy Collapse All Expand All Tritter JSON ▼ osint: v companies: **- 0:** company: "Meta" count: 1 source: "professional" **Overall Sentiment v 1:** 0 "Ntlab Italia" company: NEUTRAL 1 count: "professional" source: ₹ 2: "Effectivesoft" company: count: 1 "professional" source: Active Contributors **Contribution by Location** ₹ 3: "Utl" company: count: 1 "professional" Active | V Dead Accts | Influence source: **- 4:** "Hypersoft" company: # Contrib. Bias Risk 2. 24 1 count: source: "professional" 795,818 751,351 **- 5:** "Optirisk Systems" company: "Unknown" 513,017 count: 1 "professional" source: 44,066 <del>- 6</del>:

401 from Unknown Locations

"Ampl Optimization Inc." 1 "professional" EI.

company:

count: source:

count: email:

source:

count: email:

source: v location:

location:

source: ₹1: count:

> location: source:

location:

education: ▼ emails: <del>-</del> 0:

**- 1:** 

**∀0:** count:

₹ 2: count:

₹ 3:



"socialMedia"

1 "Menlo Park, CA" "professional" 1 "Belarus" "professional"

1 "San Francisco, CA" "professional"

source: count: 1 location: "United States" source: "professional"

600K 800K 700K

24

14

2

1

commit line 330 locations vs 401 46 26



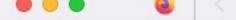


Versioning, issues, popularity, timezones, and signing

**Data Security and Control** 



	operation use_Z = False	
$\leftarrow \rightarrow$ C  localhost:5000/api/d		ost:5000/api localhost:5000/api + V
JSON Raw Data Headers Save Copy Collapse All Expand All 🛛 Filter JSON	$\leftarrow$ $\rightarrow$ C D localhost:5000/api/dire	e e e localhost:5000/apij localhost:5000/api localhost:5000, × +
<pre>▼ contributors: count: 5 dateFirstCommit: "2012-08-31</pre>	JSON         Raw Data         Headers           Save         Copy         Collapse All         Expand All              \[                 Filter JSON	$\leftarrow$ $\rightarrow$ C localhost:5000/api/direct/project/ampl $\sim_{\mathbb{C}}$ $\heartsuit$ $\checkmark$ s
<pre>&gt; list: [] sentimentMode: "neutral"</pre>	<pre>▼ contributors: count: 10 dateFirstCommit: "2012-08-31 16</pre>	JSON     Raw Data     Headers       Save     Copy     Collapse All     Expand All
signedAvg: 0 cve: null dependencies: [] projectName: "ampl/osl" "v2.1.0"	<pre>dateLastCommit: "2016-11-18 20     list: [_]     sentimentMode: "neutral"     signedAvg: 0     cve: [_]     dependencies: []     projectName: "ampl/osl"     projectVersion: "v2.5.0"     ves. Operator):     prosector the selector     x mirror to the selector     x mirror mirror x"     lect.mirror mirror x" </pre>	<pre>     contributors:         count:</pre>



Search

loc

>

Versioning, issues, popularity, timezones, and signing

localhost:

Save Copy Collapse All Expand All Trilter JSON

localhos X

rei	DOA	CTI	vit	
,				

vissues:

-

description:

name:

closedAverageDaysOpen:	191.6
closedCount:	35
closedLongestDaysOpen:	1466
closedModeDaysOpen:	0
closedShortestDaysOpen:	0
openAverageDaysOpen:	656.71
openCount:	7
openLongestDaysOpen:	1990
openModeDaysOpen:	1990
openShortestDaysOpen:	47
license:	

"GNU	General	Public	License	v3.0"
apl-	-3.0"			

openLongestDaysOpen:

1990



## Open Source Package Intelligence

description:	"GNU General Public License V3.0"
name:	"gpl-3.0"
spdxId:	"GPL-3.0"
<pre>v origination:</pre>	
isFork:	false
origin:	null
<pre>v popularity:</pre>	
downloads:	true
forks:	182
stars:	445
watchers:	43
primaryLanguage:	"C"
<pre>vullRequests:</pre>	
closedAverageDaysOpen:	15.21
closedCountMerged:	24
closedCountUnmerged:	0
-local construction	222





watchers:	43
primaryLanguage:	"C"
<pre>vullRequests:</pre>	
closedAverageDaysOpen:	15.21
closedCountMerged:	24
closedCountUnmerged:	0
closedLongestDaysOpen:	322
closedModeDaysOpen:	0
closedShortestDaysOpen:	0
openAverageDaysOpen:	805.5
openCount:	2
openLongestDaysOpen:	1581
openModeDaysOpen:	1581
openShortestDaysOpen:	30
<pre>versions:</pre>	
releaseCount:	1



JSON Raw Data Headers		
Save Copy Collapse All Expand All	₩ Filter JSON	
- 0:		
timeZone:	"-0600"	
timeZoneCount:	3	
<b>v 1:</b>		
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	
<pre>identification:</pre>	{}	
<pre>&gt; location:</pre>	{}	
<pre>&gt; osint:</pre>	{}	

### timeZoneCount: 3



## **Open Source Package Intelligence**

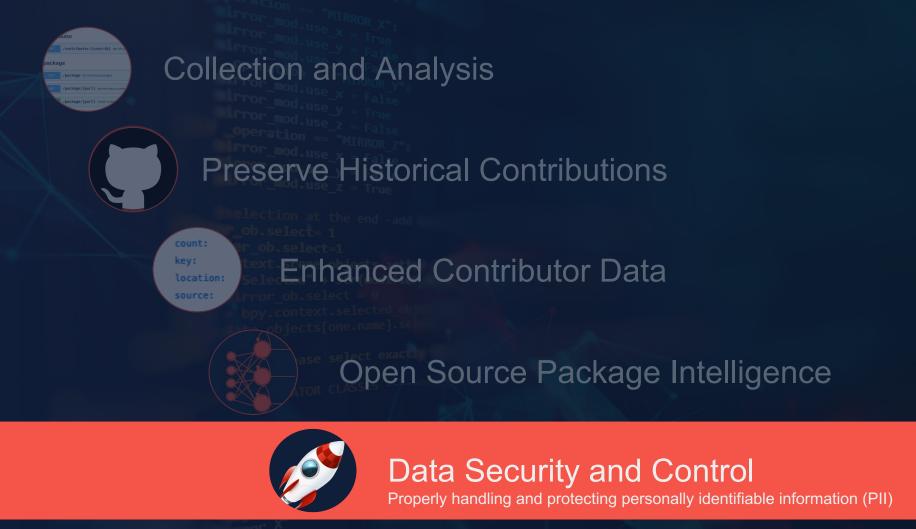
Versioning, issues, popularity, timezones, and signing

CLINCLOTICI	
timeZoneCount:	42
firstCommit:	"2016-06-14 06:25:12 +0000"
lastCommit:	"2022-02-08 18:13:29 -0600"
linesAdded:	5128
linesRemoved:	0
mergeCommitsCount:	0
<pre>identification:</pre>	{}
<pre>blocation:</pre>	{}
osint:	[]
<pre>v security:</pre>	
signed:	0.09

- OPERATOR CLASSES

LTINCZOI

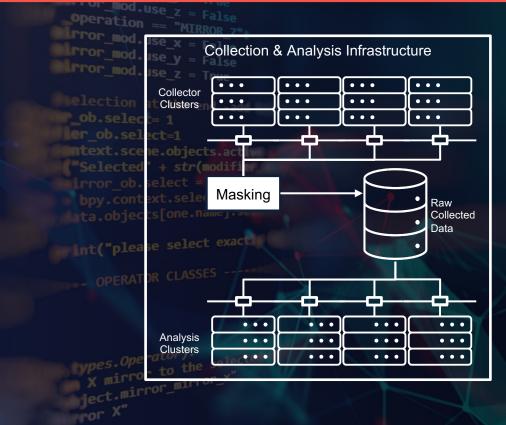
ypes.Operator): X mirror to the selectron pect.mirror\_mirror\_x" ror X"



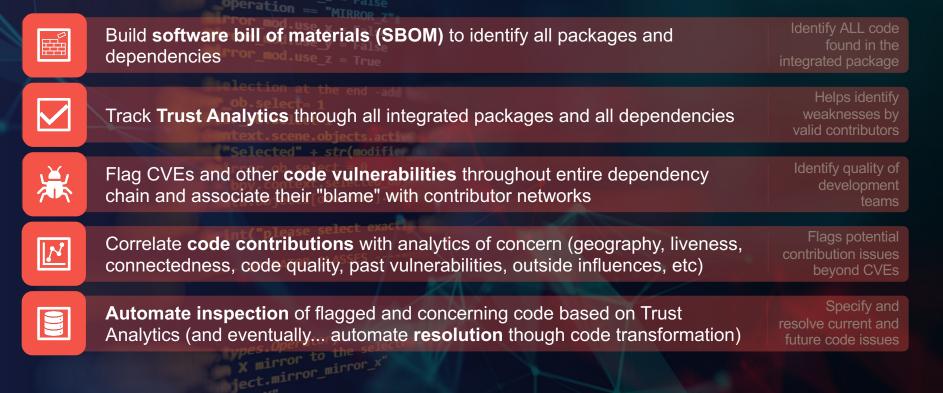


## **Data Security and Control**

Properly handling and protecting personally identifiable information (PII)







## The Solution?

TOP I



### **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.

Finally. *rust* in Open Source

INFO@DARKSKYTECHNOLOGY.COM

**DARK SKY** TECHNOLOGY

mirror mod.use x drror mod.use y

operation == "M]

vject.mirror.mir

Pror Y