## default">

media-body">

ss="media-heading">Media



ss="media-object

MAKING CODE SCANNING AS EASY AS SPELL CHECK™

## INTRODUCTION

The world is turning to code. Your car, your house, and your business are all running on code. Can that code be hacked?

The Yes: 48% of code is never scanned.<sup>1</sup> With 111 billion lines<sup>2</sup> of code written every year there is a massive gap in security because the remaining code is scanned infrequently and has significant issues.

We see the results every day in the news. In 2019, the companies hacked include social networking WhatsApp to investment group BlackRock.<sup>3</sup> A hacker just added malicious code to steal bitcoin, effecting 2,000,000 users, using a popular open source library.

#### WHY IS THIS HAPPENING

Current code scanning solutions are:

**Too Expensive:** Significant cost across people, process, and technology to implement. **Too Complicated:** Involved infrastructure, configuration, & integration. **Too Regimented:** Doesn't answer basic questions and requires complicated workflows.

Nucleaus<sup>™</sup> is Democratizing Application Security<sup>™</sup> by making code scanning available to everyone, with zero barriers to entry.

### WHAT IS THE IMPACT ON BUSINESS?

Loss of Revenue: Some vulnerabilities can lead to direct financial impact like Point of Service (POS) or WebApp attacks.

Loss of Trust and Reputation: Data breaches and security holes can expose customers, clients and employees.

Legal: A growing trend to legal action on behalf of customers and clients from data breaches.

<sup>1.</sup> Veracode

https://www.csoonline.com/article/3151003/world-will-need-to-secure-111-billion-lines-of-new-software-code-in-2017.html 2. 3.

https://www.identityforce.com/blog/2019-data-breaches

## CHALLENGES WITH EXISTING CODE SCANNING SOLUTIONS



Current code scanning solutions are complicated and difficult to use and time consuming to setup. It takes an expert in that system to understand the output. Because of the complexity they are used only on an as need basis, usually upon release. New vulnerabilities are identified daily and if you don't scan your old code you won't know if you are at risk of new threats. Current solutions are:

**Complex to setup** - Require dedicated teams inside of organizations to manage the tools and current teams of engineers are needed to setup.

**Difficult to decipher results** – The results are complicated and take time to understand what is most important.

**Repetitive incidents** – Each vulnerability creates multiple incidents and the repetition of results creates a waste of time repeating tasks.

**Lacking historical data** – Code and vulnerabilities evolve over time. Understanding how your systems are improving or declining is critical to maintain secure system.

**Not up to date** – Code is typically only validated and scanned at release but new vulnerabilities are found daily. If a critical vulnerability is found it is important to fix in a timely fashion.

**Expensive** – Licenses are expensive and limited in scope. Current users strive to limit the total number of scans at the expense of transparency.

Nucleaus<sup>™</sup> offers a solution that makes code scanning easy and provides a level of transparency that reveals the problems that can lead to a security breach.

## WHY NUCLEAUS™?

Nucleaus<sup>™</sup> is **Simple, Approachable, Affordable and Actionable**. We are making code scanning as easy and approachable as Spell Check. We are providing a solution not a technology.

The Nucleaus<sup>™</sup> dashboard provides up to date information on all code repositories and can alert immediately when a critical vulnerability occurs.

**Continual Updates** - We continuously update and scan repositories after they are added. Yesterday's scan is already outdated due to new vulnerabilities. Nucleaus<sup>™</sup> automated continuous vulnerability updates provides up-to-the-minute results.

**Code Issue and Project Dependencies** – Easy to identify, prioritize and fix issues whether from code or project dependencies.



### NUCLEAUS<sup>™</sup> KEY BENEFITS:

Simple, Approachable, Affordable and Actionable: 30 min to get setup and running.

**Continuous updates:** Continuously update and scan repositories after they are added.

**Automated:** The platform operates autonomously, scanning repos and delivering results. There are only two things you can do: add additional repos and run ad hoc scans.

Scale: Scan 1 repo or 1,000's automatically everyday with no human intervention.

**Portable:** Access Nucleaus<sup>™</sup> dashboard from anywhere, including your phone.

# 9 LANGUAGES & 72 FRAMEWORKS

#### GETTING SMARTER EVERYDAY

Conservatively, Nucleaus<sup>™</sup> supports 9 of the most popular languages on Github and 72 frameworks such as:

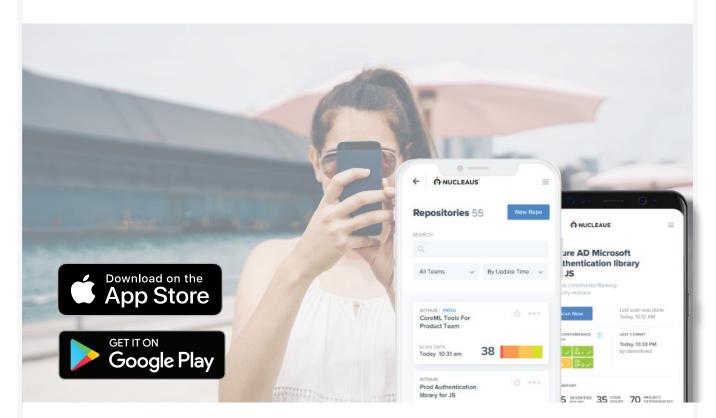
JavaScript Flex Go (GoLang) Java TypeScript NodeJS PHP Python Ruby

and continuing to add languages on a regular cadence...



## **APP SCREENSHOTS**

# Result-Driven from Cxo to Dev from anywhere with the Nucleaus<sup>™</sup> App



#### Dark Mode and Light Mode Nucleaus<sup>™</sup> Console:

WCAG accessibility was taken into consideration with dark mode to ensure a sufficient contrast ration for folks with visual disabilities.

• NUCLEAUS		ashboard 🗮 Repos				
			-O-NUCLEAUS	📿 Deshb	ored 🗏 Repos 🗘 integrations	Account 2
<b>Repositories</b> 1	10			Dashboard		
Repusitories	10		ACTIVE REPORTORIES	SEVENTIES TOTAL	SEVERTIES THAT	2 4
			5 401	2 980	2 306	August 15th, 2019 2 5:
		ime 🗸				Cerective Seventiles
			Severities Overview			
	github.com / thirden /			-		June 10 - 16
11	aming-security-mistake		Top 10 Repos	Seven est	854 MAY DAY	
ытнив 🏠	ытнов С	GITHUB	Facebook Node JS (20) Facebook Node JS (20) Facebook SDX (20) Face		June 12, 2019. 780 issues	_
Facebook NodeJS Business SDK	Azure AD Microsoft Authentication library	Apple iCalendar lib used by		IN AVERAGE PER		
Business 3DK	for JS	CalendarServer	Apple Calendar Ib 00 Ap bidd by 00 Ap Filming Seculty 00 Pil Pilming Seculty 00 Pil	Int by 85% Int by KIPOS HEYE Refer and LESS THEN 10 SUBJECT		
				sevences		
			Code			⇒
SCAN DATE Today 10:31 am	SCAN DATE Today 10:31 am	SCAN DATE Today 10:3	BRANCHES	COMMITS (5)	сонтвентова (2)	LINES OF CODE
105	1031	STATUS Scan Fa	10 045	322 054	18	208 862 450
		000 /9	size or cope	LANGUAGES	REPOSIN CONFORMANCE	PELLASE
		6	33	12	5 340	120
ытнив 🖒 Flaming Security	ытн∪в ☆ Flaming Security	ытнив Azure AD Microsoft	Compensating Control Recommendations			$\leftrightarrow$ $\rightarrow$
Mistake and Flaming	Mistake and Flaming	Authentication library		10	18	22
again	again	for JS	25 Brood with Framework	Repos with OWASP Top 10 Vulnerabilities	Repos with Config files	Repos with Compliance Issues
			upprades		•2	(30)
			Show Repos	Show Repos	Show Repos	Show Repos

## **RESULTS IN THREE STEPS**

Simple: Nucleaus<sup>™</sup> makes code scanning as easy as doing a spell check.

**Democratized:** No barriers to entry, skills, or technology.

Approachable: Anyone, on any device, can understand risk and how to remediate.



Critical priority	5	High	5	Medium	10	Low	8
Denial of Service		BUG : TLSSocketEvent.as	A1	BUG : TLSSocketEvent.as	A1	BUG : TLSSocketEvent.as	A1
Cross-Site Scripting		Cross-Site Scripting (XSS)		Cross-Site Scripting (XSS)		Cross-Site Scripting (XSS)	
Code Execution thro IIFE	ough A5	BUG : SSLEvent.as		BUG : SSLEvent.as		BUG : SSLEvent.as	
DoS due to excessiv large websocket me		DoS due to excessively large websocket message		DoS due to excessively large websocket message		DoS due to excessively large websocket message	
		Code Execution through IIFE		Code Execution		Code Execution through	
Code Execution thro IIFE	ough A1			DoS due to excessively large websocket message		DoS due to excessively	

Making Code Scanning As Easy As Spell Check<sup>™</sup> 7

## WHICH OF THE FOLLOWING CAN YOU ANSWER TODAY?

ELEPHANT IN THE ROOM.

#### **Dev Team:**

- Which repository has the most risk?
- How do you prioritize vulnerabilities?

#### CISO/CIO/CTO:

- How many total critical, high, medium and low vulnerabilities do we have?
- Are the vulnerabilities trending up or down?

#### CEO/ Board:

• Do those vulnerabilities pose a **risk** to our brand and customers?

## As the landscape of threats increases, CISOs, secrity committees, executives and boards of directors are demanding meaningful information for decision-making.

Cyber security stakeholders face significant challenges identifying, obtaining, processing and aggregating key information that enables them to steer towards defined targets effectively, and ultimately be in better control of their organization's cyber security.



https://nucleaus.com hello@nucleaus.com 800.609.0393