



# DelphiDay

italian conference

## DerScanner

Delphi App Security



# PAOLO ROSSI

## WINTech ITALIA - CTO



[blog.paolorossi.net](https://blog.paolorossi.net)



[paolo@paolorossi.net](mailto:paolo@paolorossi.net)



[twitter.com/awebguy](https://twitter.com/awebguy)



[github.com/paolo-rossi](https://github.com/paolo-rossi)



[linkedin.com/in/paolo-rossi-pc](https://linkedin.com/in/paolo-rossi-pc)



# DelphiDay

italian conference

11-12 Giugno 2024  
Piacenza



wintech  
italia





# GITHUB PROJECTS



[github.com/paolo-rossi](https://github.com/paolo-rossi)



## Delphi JWT

JSON Web Token Library



## WiRL

REST Library for Delphi



## Linux Daemon

Real Linux daemons



## Delphi Neon

JSON Serialization Library



## OpenAPI-Delphi

OpenAPI 3.0 Library



## NATS Delphi

NATS Client Library for Delphi



# AGENDA

---

1. Defining Security
2. Risks, Threats, and Vulnerabilities
3. Laws, GDPR and Application Security
4. Designing a security strategy
5. DerScanner
6. DerScanner for a Delphi developer



# Your Security?

What is your security level?

0



# WHAT IS YOUR SECURITY?

**NO SECURITY**

**FCS SECURITY  
(FINGER CROSSED SECURITY)**



# Defining Security

# 1



# DEFINING SECURITY

- Protection of internet-connected systems
- Being protected in cyberspace means
  - ◆ Protect computer systems against unauthorized access or attack
  - ◆ Protect networks and devices from cybercrime
  - ◆ Protect data from data breaches
  - ◆ Protect applications against unauthorized access misuse





# WHY IT'S IMPORTANT

## Cost of a Data Breach Report 2022 (IBM)

- ◆ 83% of organizations studied have had more than 1 data breach
- ◆ 60% of breaches led to increases in prices passed on to customers
- ◆ 45% of the breaches were cloud-based
- ◆ 19% of breaches caused by stolen or compromised credentials





# COSTS OF DATA BREACH

2  
Middle East  
2022 \$7.46

1  
United States  
2022 \$9.44

3  
Canada  
2022 \$5.64

5  
Germany  
2022 \$4.85

4  
United Kingdom  
2022 \$5.05

6  
Japan  
2022 \$4.57

8  
Italy  
2022 \$3.74

7  
France  
2022 \$4.34

9  
South Korea  
2022 \$3.57

Measured in USD millions



# Risks & Threats

Risks, Threats & Vulnerabilities

# 2



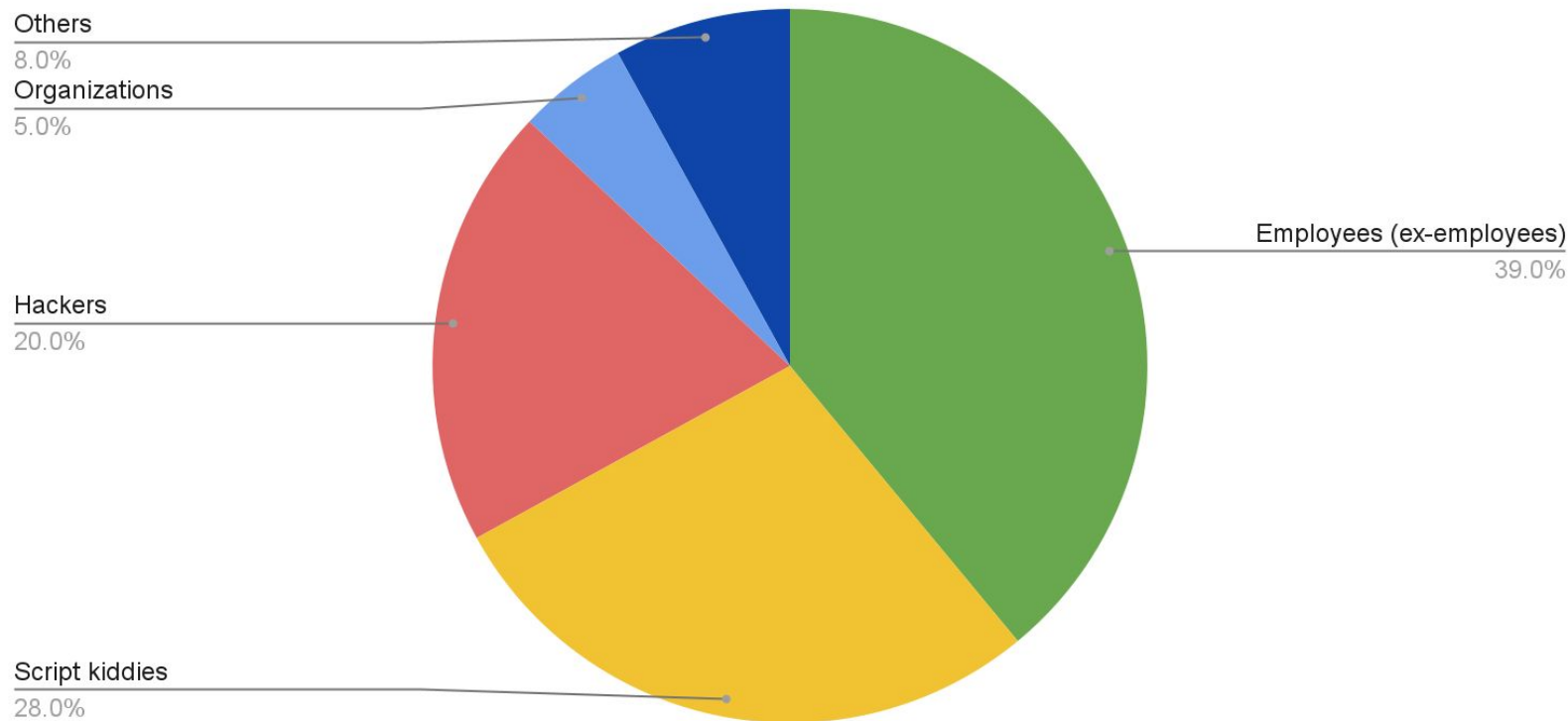
# THREAT'S SOURCES

- Where the attackers come from?
- You absolutely need to know
  - ◆ In order to build defences in the right places
  - ◆ In order to choose the type of defence

CARE TO GUESS?



# Threats source among organizations

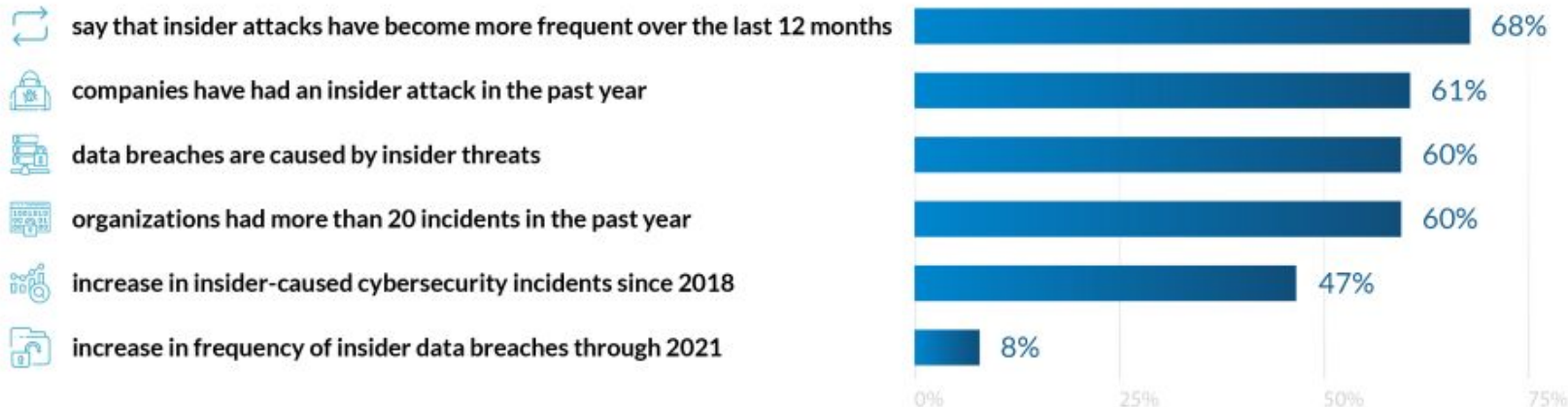




# INSIDER THREAT STATISTICS

## 1 Insider Threat Frequency of Attacks

Sources: Goldstein, CyberSecurity, ObservelT, Shey, Bitglass, IBM







# INSIDER THREAT STATISTICS

## 2 Top Motivations for Insider Attacks

Source: Fortinet



fraud



monetary gain



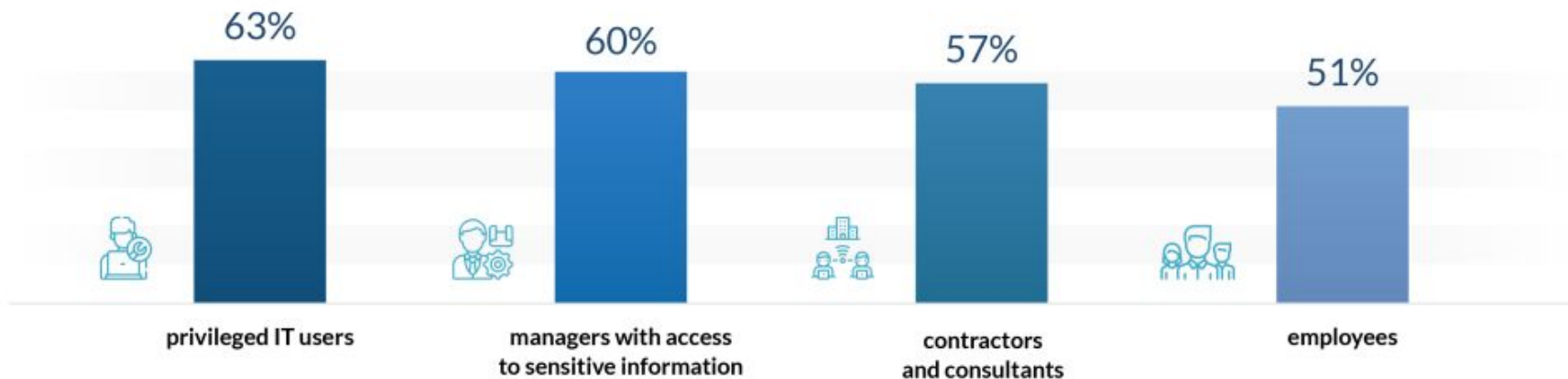
IP theft



# INSIDER THREAT STATISTICS

## 3 Top Insider Threat Actors

Source: Cybersecurity Insers, Bitglass





# Laws & Security

GDPR, Laws & Security

# 3



# GDPR

- Introduced on 25 May, 2018
- Encourages organizations to properly handle user data and privacy
- Those not in compliance can face fines
- In the past years, this has resulted in more than \$1.4 billion USD in fines levied against tech giants, hotels, governmental agencies, and violators in other sectors.



# GDPR REQUIREMENTS

- Enhanced application security
  - ◆ End-to-end encryption, multi-factor authentication, and so on
- Facilities for users to exercise their data privacy rights
- Quick data purge at a user's request
- Users given access to data collected from or about them
- Consent from users about what data is obtained and how it's used



# SECURITY & GDPR

- GDPR can feel like a threat
- If used properly, GDPR can help you
  - ◆ It's a term that every manager knows
  - ◆ Bigger security budget
  - ◆ More security integrations
  - ◆ Faster response to security incidents





# APPS & GDPR

## → Data collection

- ◆ Is there a good reason for collecting this data?
- ◆ Has the collection of non-necessary data been minimized?
- ◆ Does the user consent to the collection of this data?

## → Data breach

- ◆ Have you informed supervisors within seventy-two hours of the breach?
- ◆ Have you carried out a data protection impact assessment before adopting new technology that interacts with user data?



# APPS & GDPR

## → Data protection

- ◆ Have you taken adequate measures to prevent compromise of user data?
- ◆ Are your cybersecurity policies and measures up to date?
- ◆ Is personally identifiable information (PII) of users properly encrypted to prevent abuse by malignant actors?

## → Data transfer

- ◆ Is the data transfer handled in a way that doesn't compromise data?
- ◆ Does the receiver have enough security in place to protect data?



# APPS & GDPR

## → Data rights

- ◆ Do users have the ability to request copies of their data?
- ◆ Do users have the ability to object to certain uses of their data?
- ◆ Can you delete a user's data immediately if they request it?
- ◆ Does this include removing their data from your backups?



# Defense Strategy

Designing a Security Strategy

# 4



# DETECTION TOOLS

- SAST: Static Application Security Testing
- DAST: Dynamic Application Security Testing
- IAST: Interactive Application Security Testing
- SCA: Software Composition Analysis



# SAST

- Static Application Security Testing
- Code analysis on the source code looking for security issues
  - ◆ Example: Plain Text Passwords or Keys hardcoded
- Language-dependant
- Mostly as IDE plugins
- I don't know anything specific for Delphi (Pascal Analyzer?)





# DAST

- Dynamic Application Security Testing
- DAST tools
  - ◆ Scan the application from the outside
  - ◆ Examine the application in its running environment
  - ◆ Manipulate the application in order to discover security vulnerabilities
- Language independent



# IAST

- Interactive Application Security Testing
- Combines the strengths of SAST and DAST
- Assesses the application from within, instrumenting the code
  - ◆ Through a library to compile with the application
- Language dependant



# SCA

- Software Composition Analysis
- Not all code is actually written by a developer
  - ◆ You probably use some libraries in your application
- Usually SCA tools scan open source libraries
- Language dependant



# PENETRATION TESTING

- The right tool used by the right person
  - ◆ Usually performed by skilled security professional
- Internal penetration tests (performed by a red team)
- External penetration test (performed by an external party)



# DerScanner

# 5

# DerScanner

A complete application security testing solution  
to eliminate known and unknown code threats



# The digital transformation has made application development 10x more agile

## Frequent Changes and Fast Paced

Agile development focuses on rapid iterations and frequent changes to the codebase. This fast-paced environment can lead to security being overlooked or given lower priority in the rush to meet release deadlines.

## Lack of Comprehensive Planning

Agile methodologies often lack the long-term planning seen in traditional development models. This can result in security considerations being an afterthought rather than being integrated into the initial design.

## Integration of Third-Party Components

Agile development often involves integrating multiple third-party components rapidly. These components can introduce vulnerabilities if they are not properly vetted or kept updated.

# Due to deadlines, developers are taking shortcuts

## Hardcoded Secrets

Embedding passwords, API keys, or encryption keys directly in the source code, which can be easily extracted by malicious actors.

## Insecure Data Storage and Transmission

Overlooking the need for encryption of sensitive data both at rest and in transit.

## Backdoors

Implementing hidden entry points in the code to facilitate easier access or debugging, which can be exploited by attackers.

## Insufficient Input Validation

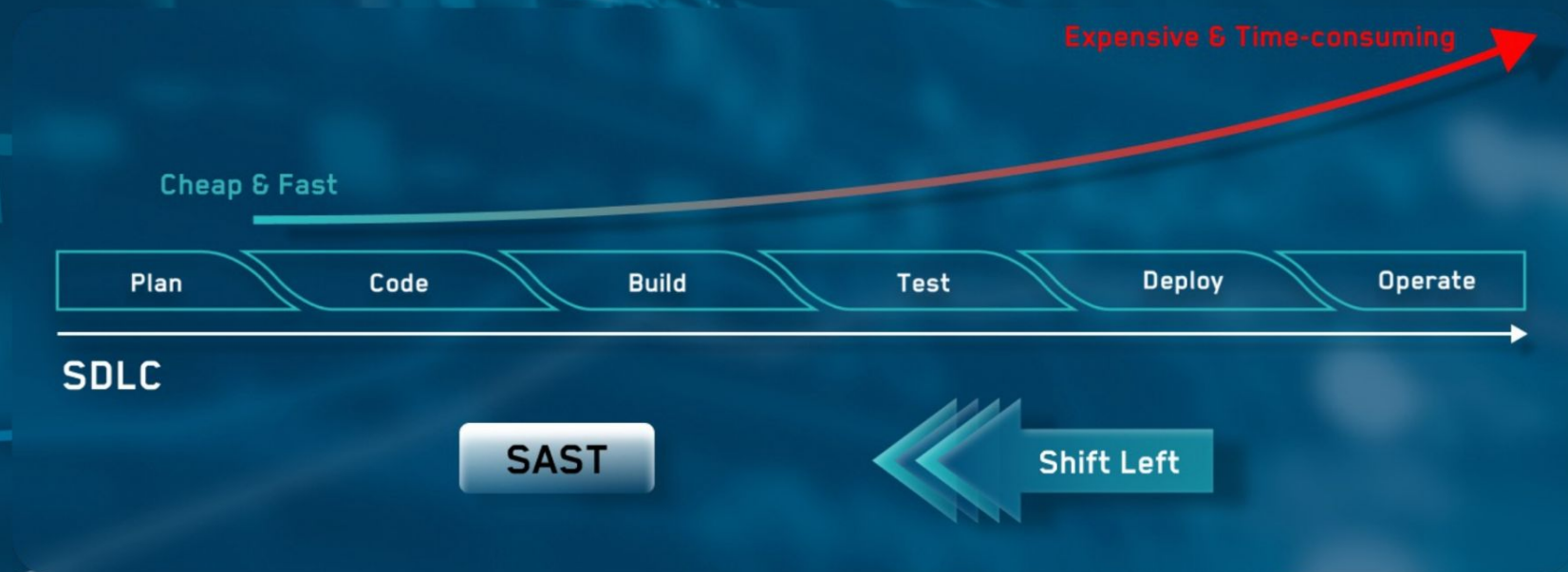
Failing to thoroughly validate user input can lead to vulnerabilities like SQL injection, cross-site scripting (XSS), and buffer overflows.

## Unverified open-source or third-party components

Embedding packages downloaded from the Internet without conducting any security pre-checks, which can introduce vulnerabilities or malicious code into the application.



# Cost of Fixing an Application Vulnerability



# Start with Early Detection of Known Vulnerabilities

Shift security left by Implementing Static Analysis early in the development pipeline  
Scan the application's source code to identify patterns that match known vulnerabilities.

## SDLC



**SAST**

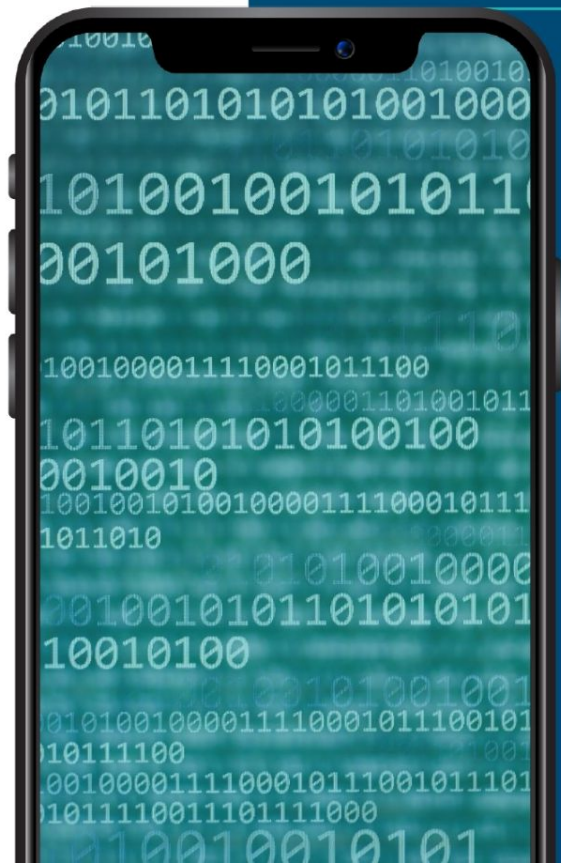
- ✓ Hardcoded secrets
- ✓ Backdoors
- ✓ SQL injections
- ✓ Cross-site scripting (XSS)
- ✓ Buffer overflows
- ✓ and more

**Shift Left**

# A Single Solution for 43 Popular Languages



The source code can be analyzed [from uploaded files](#) or directly [from the repository](#).



# Integrate Security Checking in your SDLC

By integrating **DerScanner** with major developer tools, you can perform source code checks early in the pipeline.

## Repositories



## VCS hostings



## Development environments IDE



*Coming soon!*



## CI/CD servers



## Bug tracking



## Code analysis



Open API (including **JSON API** and **CLI**) provides powerful integration and automation options



# Scan Binaries When the Source Code is Unavailable

## Legacy Applications

Assess and mitigate vulnerabilities where source code might be lost, outdated, or poorly documented.

## Compliance and Audit

Ensure the compiled application complies with security regulations in compliance strict industries

## Identify Exotic Vulnerabilities

Discover harmful vulnerabilities that might not be detectable through source code analysis

# Unveil the Unseen, Secure the Undiscovered

## 1. Upload your application in any available format

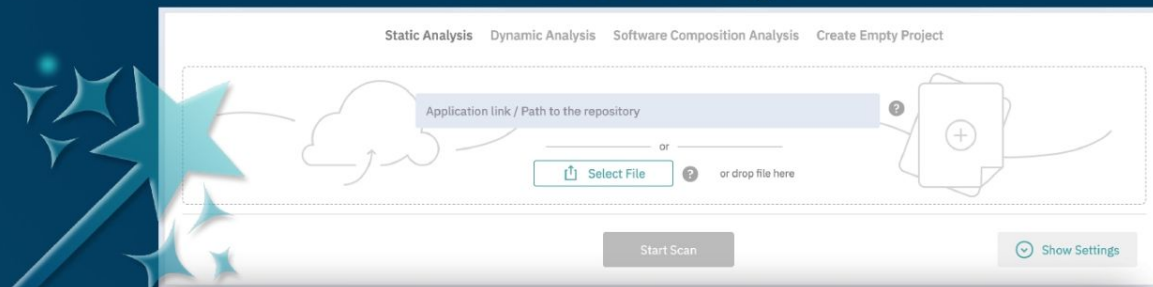


<https://play.google.com/store/apps/AppName>



<https://apps.apple.com/en/app/AppName>

## 2. Science and Magic



## 3. Get security assessment results



# Pass Compliance Assessment with Ease

Depending to your industry, various regulatory standards require security testing of operational applications.

Get a vulnerability report to ensure your code is compliant to:

- PCI DSS
- OWASP
- HIPAA
- CWE/SANS Top 25



## *Certificate of CWE™ Compatibility*

*DerSecur Ltd.'s  
DerScanner*

*In accordance with the Requirements and  
Recommendations for CWE Compatibility,  
version 1.0, the CWE Program hereby awards the  
label of CWE-Compatible  
as of 7 June 2022.*

# You can't Restrict Developers from Using Third-party Components

But you still can prevent the open-source driven risks

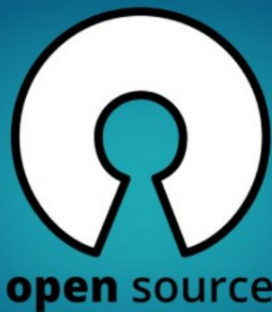
## Visibility into Open-source

Gain visibility into open-source components and dependencies to detect known vulnerabilities before they become exploitable.

## License Compliance

Ensure that the open-source licenses of used components are compatible with the project's licensing terms to avoid legal issues.

## Software Composition Analysis (SCA) for



## Mergers and Acquisitions (M&A) Due Diligence

Assess the software assets of the target company, providing insights into potential risks, liabilities, and the quality of the codebase.



# Ensure Confidence in Open-source Components

If they had Software Composition Analysis (SCA) in place during the famous attacks

## Heartbleed Bug in OpenSSL (2014):

This was a severe vulnerability in the OpenSSL cryptographic library, affecting millions of websites.

SCA could have identified the vulnerable version of OpenSSL being used in applications and prompted an update to a patched version.

## Equifax Data Breach (2017):

This breach occurred due to an unpatched Apache Struts framework used by Equifax.

SCA could have flagged the outdated framework and facilitated timely updates, potentially preventing the breach.

## SolarWinds Orion Software Hack (2020):

In this sophisticated supply chain attack, malicious code was inserted into the software's build process.

SCA would monitor changes in component behaviour or integrity and would have raised red flags about unauthorized modifications.

## Apache Log4j Vulnerability (2021):

Known as Log4Shell, this critical vulnerability in the widely used Log4j logging library allowed remote code execution.

SCA would have identified the vulnerable Log4j versions in software inventories and recommended urgent updates.

# Find Unknown Vulnerabilities with Supply Chain Security

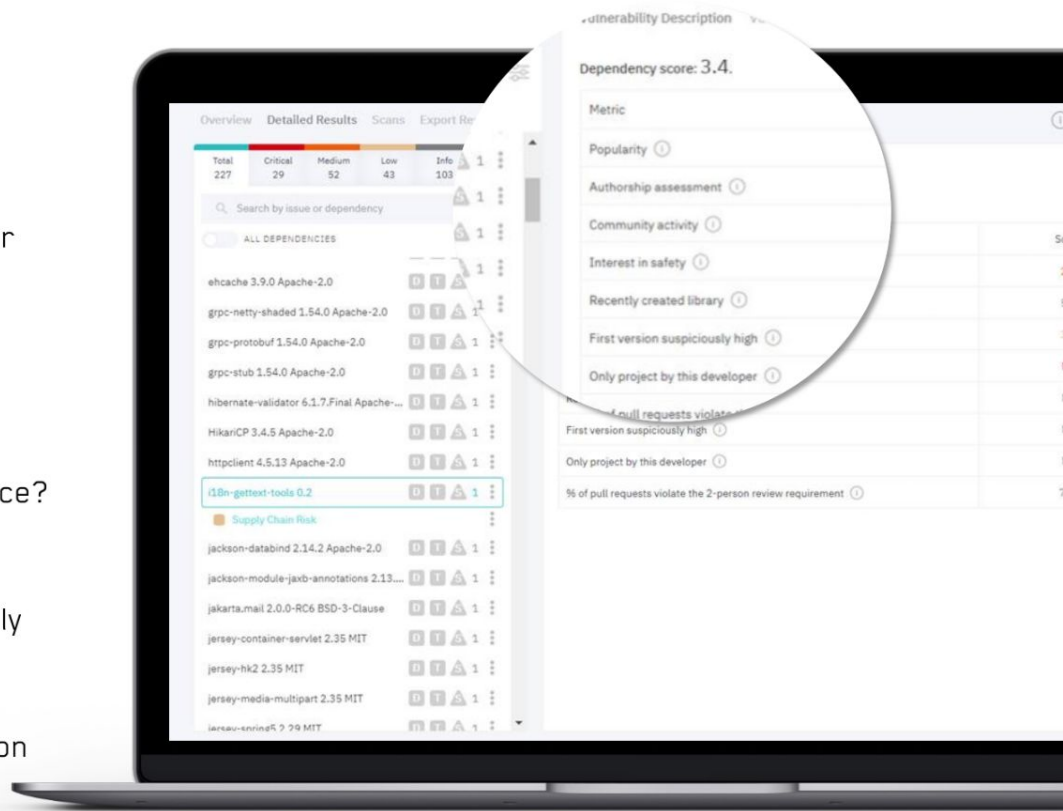


DerScanner continuously assesses GitHub repositories.

Check any package's reputation and make an informed decision about whether to use it in your application.

Get any package scored and learn:

- How popular is the package?
- Is the author trusted?
- How active is the community maintenance?
- Did the author enable basic security?
- When was the library created?
- Was the first library version suspiciously high?
- Is it the only project by the author?
- Do the pull requests pass the two-person authorization?



# Remediate Known and Unknown Code Threats across SDLC

- Protect any application from both **known** and **unknown vulnerabilities**
- **Integrate** security checks in your SDLC to sync development and security efforts

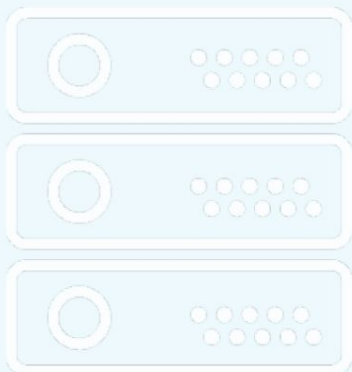


# Deployment Options

## On-premise

### Hosted by you

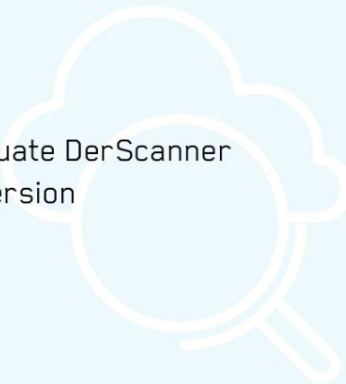
- Absolute privacy



## SaaS

### Hosted by us

- Fastest way to evaluate DerScanner
- Always the latest version



# Why Customers Choose DerScanner

## Single AppSec Platform

- ✓ Natively integrated major application security technologies
- ✓ Detects correlation for the full context of what issues matter the most

## Low False Positives

- ✓ Proprietary Fuzzy Logic technology to set the threshold of alerts that suits your priorities best

## Industry Recognized

- ✓ Recognized by Forrester among leading SAST vendors
- ✓ CWE certified by MITRE
- ✓ Highly rated by customers on G2

**MITRE FORRESTER®**



## Security Friendly Reports

- ✓ Reports are written in simple language that a security professional with no development experience can understand

## Best for Security Audits

- ✓ Even if the source code is not available, check running web and mobile apps or legacy apps with a combination of binary SAST and DAST

## Traditional Technical Support

- ✓ No bots. Only classical people-powered support
- ✓ Messenger chat support for Enterprise customers



Thank you for you time!

Learn more: <https://derscanner.com/>

Drop us a line: [company@dersecur.com](mailto:company@dersecur.com)





**Demo:**

# DerScanner

---

- SAST with Delphi
- Settings
- Reporting







# DerScanner Licenses

6



# LICENSE SCHEME

## → Scan as You Go

- ◆ 36 languages | 1 user | Per Scan Pricing | Cloud | No integrations

## → Flex

- ◆ 3 Languages | 1 User | Unlimited Scans | On-premise | SDLC integrations

## → Enterprise

- ◆ 36 languages | Unlimited Scans | Unlimited Users | On-premise | SDLC integrations

Through Wintech Italia



# SCAN AS YOU GO

- SAST | DAST | SCA | SCS
- 36 languages | 1 user | Per Scan Pricing | Cloud
- Suited for scanning the source and having a report
- Not suited if you want to add security to your SDLC



# FLEX

- SAST
- 3 Languages | 1 User | Unlimited Scans | On-premise
- Suited for adding security to your SDLC
- Quite expensive
- With 3 languages (more as options) you can cover all your development needs
  - ◆ For Example: Delphi, JavaScript, C#
- You can buy DAST and SCA scans



# ENTERPRISE

- SAST | DAST | SCA | SCS
- 36 languages | Unlimited Scans & Users | On-premise
- Suited for adding security to your SDLC
- Complete solution for all your security needs
- Expensive



# AS A SERVICE

- The hard work is not scanning your source
- The hard work is to fix the vulnerabilities in your source code!
- You need a guide through the entire process
- **Partnership DerScanner & Wintech Italia**
- In September we will be ready with our offer
  - ◆ Training
  - ◆ Reselling Licenses
  - ◆ Selling Services



THANK YOU