BuffaLogs

Authentication protection

Who we are

Federico Foschini

Threat detection team leader at Certego

GSoC mentor for Honeynet

Lecturer Master of cybersecurity UNIBO

Lorena Goldoni

Threat Detection Engineer at Certego & Master student

Principal Maintainer of BuffaLogs - open source project

certego

How BuffaLogs started

In Certego we are deeply committed to contributing to the open source community.

As detection specialists we decided to develop a new detection tool and we asked ourselves:

"What is the most valuable tool we could contribute?"

Our criteria:

- Broad impact: must solve real problems for most security teams
- Innovation: fill an existing gap in the security landscape
- Sustainability: manageable by a small dev team

certego

Identifying the right focus for our tool

Reviewing and evaluating existing products

Reviewing security incident we managed

certego

Product evaluation

How can we evaluate a product?

Every vendor claims perfect detection

Qualys Security Blog
Qualys Achieves 100% Major Step Detection in the 2024 MITRE ATT&CK Evaluations, Enterprise
In today's rapidly evolving threat landscape, ransomware continues to dominate as one of the most significant cybersecurity challenges.
3 weeks ago

Emsisoft
Emsisoft Enterprise Security + EDR Achieves 100% Detection in AVLab's September 2024 Test
In this rigorous test, Emsisoft Enterprise Security + EDR blocked all 510 malware samples, achieving a flawless 100% detection rate.
29 Oct 2024

Acronis
Acronis Advanced Security + EDR wins SE Labs Enterprise Advanced Security Award
SE Labs, an AMTSO member and independent, UK-based testing laboratory evaluated Acronis Cyber Protect Cloud with Acronis Advanced Security +...
1 Jul 2024

CrowdStrike
CrowdStrike Falcon Wins Best EDR Annual Security Award in SE Labs Evaluations
The CrowdStrike Falcon platform has received the best Endpoint Detection & Response 2024 award from SE Labs for the third consecutive year.
12 Apr 2024

SentinelOne
Mitre Attack Evaluations – SentinelOne Achieves 100% Protection and Detection

Microsoft
Microsoft Defender XDR demonstrates 100% detection coverage across all cyberattack stages in the 2024 MITRE ATT&CK® Evaluations: Enterprise
For the sixth year in a row, Microsoft Defender XDR recognized in the independent MITRE ATT&CK® Evaluations: Enterprise.
3 weeks ago

GlobeNewswire
Check Point Infinity XDR/XPR Achieves 100% Detection Rate in 2024 MITRE ATT&CK® Evaluations
Check Point Infinity XDR/XPR Delivers Unmatched Protection Against Ransomware and Endpoint Threats...
3 weeks ago

Sophos News
Sophos excels in the 2024 MITRE ATT&CK® Evaluations: Enterprise
Spoiler alert! Sophos has once again achieved exceptional results in the latest 2024 MITRE ATT&CK Evaluations for Enterprise.
3 weeks ago

KXAN Austin
Sophos XDR Excels in MITRE ATT&CK® Evaluations: Enterprise
100% of Sophos XDR detections for adversary activities targeting Windows and Linux devices provide rich analytic coverage and achieve the...
3 weeks ago

itvoice.in
Trend Micro Achieves 100% Coverage Rate in MITRE ATT&CK® Evaluations
Global cybersecurity leader Trend Micro Incorporated announced its exceptional scores in the latest round of the MITRE ATT&CK® Evaluations.
2 weeks ago

Sophos News
Sophos named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms
The Gartner® Magic Quadrant™ for Endpoint Protection Platforms provides readers with a comprehensive evaluation of the industry's most...
23 Sept 2024

CrowdStrike
CrowdStrike named a Leader by Gartner
CrowdStrike has been named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms for the fifth consecutive time.
1 Oct 2024

Microsoft
Microsoft is named a Leader in the 2024 Gartner® Magic Quadrant™ for Endpoint Protection Platforms
We are excited to announce that Gartner has named Microsoft a Leader in the 2024 Gartner Magic Quadrant for Endpoint Protection Platforms for the fifth...
25 Sept 2024

ChannelLife Australia
Trend Micro leads Gartner's endpoint security magic quadrant
Trend Micro has been placed in the Leaders' Quadrant of the 2024 Gartner Magic Quadrant for Endpoint Protection Platforms (EPP).
25 Sept 2024

SentinelOne
A Gartner Magic Quadrant Leader for Three Consecutive Years
For the third year in a row, SentinelOne has again been recognized as a Leader in the 2023 Gartner Magic Quadrant for Endpoint Protection Platforms.
17 Jan 2024

Trend Micro
Endpoint Gartner Magic Quadrant 18-Time Leader in 2024
Trend Micro is honored again to be named a Leader in the latest Gartner Magic Quadrant for Endpoint Protection Platforms.
22 Jan 2024

certego

Every vendor claims perfect detection

Has Infosec problem been solved? No, it's gotten harder

Infosec research council hard problems list (2005)

- Global scale identity management
- Insider threat
- Availability of time critical systems
- Building scalable secure systems
- Attack attribution and situational understanding
- Information provenance
- Security with privacy
- Enterprise level security metrics

20 years later we also have:

- More complexity
- Long tail of old technologies with new technologies
- Wider use cases by broader enterprise/consume base
- Ripple effects of breaches
- Monetization of data
- Kinetic effects of cyber attacks

Source: Wendy Nather

certego

What we observed: Kill chain

Initial Access

Vectors:
- Spear-phishing
- Zero Day
- Trojan
- Known Vuln.
- Supply chain

Enrollment

Connections:
- Agent to C & C

I'm alive!

Reconnaissance & Lateral Propagation

Connections:
- Agent to C & C

Weaponize

Connections:
- C & C to Agent

Attack

Connections:
- Agent to C & C

Seconds

Minutes

Hours

2-3 Days

3-4 Days

certego
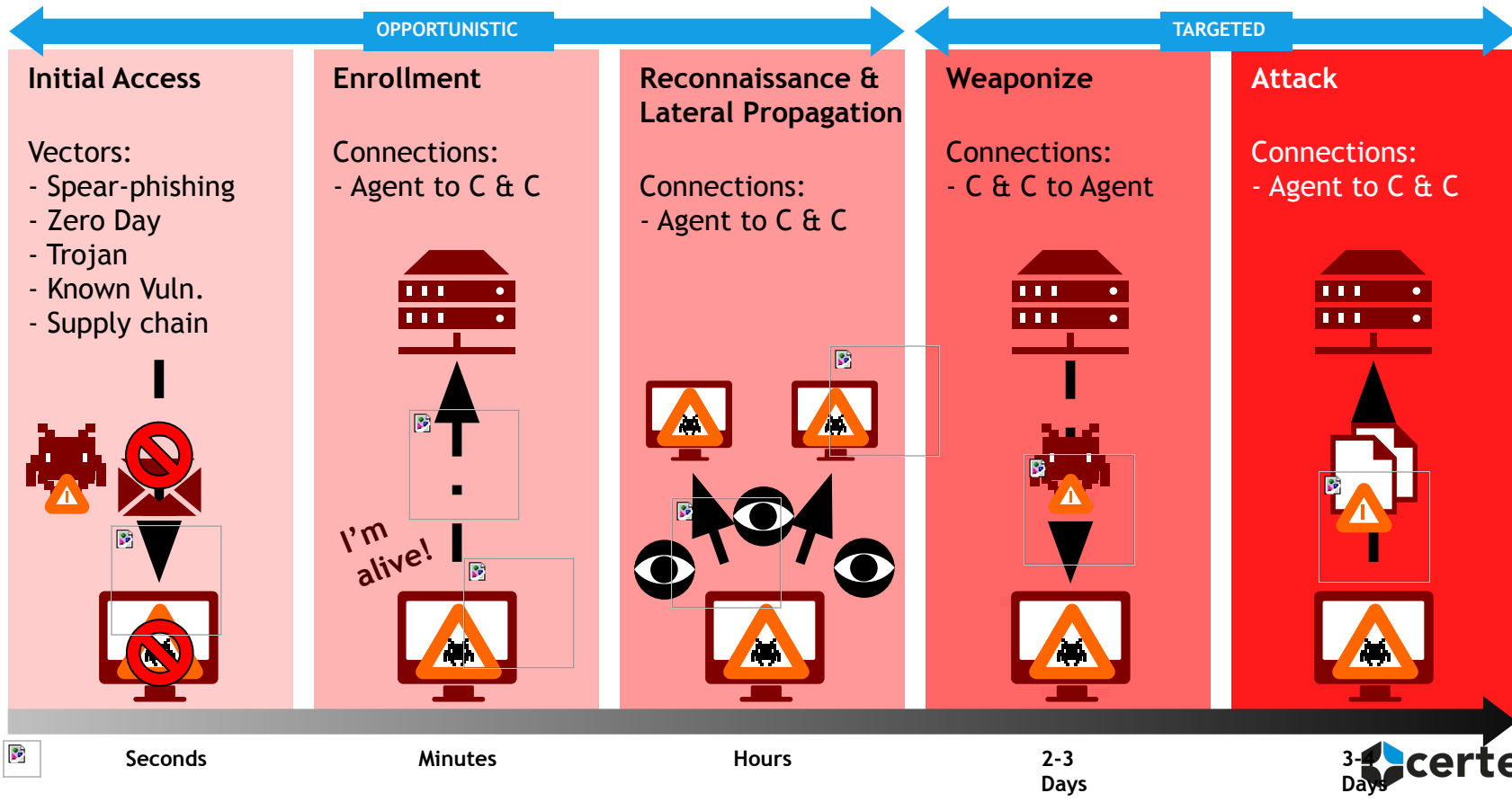
What we observed: Security Incidents 2023-2024

10 Major Compromises:

Initial Access:

- 1 Bruteforce
- 2 Phishing campaigns
- 7 Compromised valid credentials

Key Attack Patterns:

- Remote Access Abuse
  - Consistent foreign IP login attempts
  - VPN and remote access tools exploitation

- Post-Compromise Activities
  - Lateral movement
  - Data encryption
  - Reverse shell deployment
  - Cryptocurrency mining

certego

What we obs... 23-2024

10 Major Compromise... erns:

Initial Access:

...ccess Abuse

- 1 Bruteforce
- 2 Phishing camp...
- 7 Compromised ...

...nt foreign IP login attempts
...remote access tools
...ion

...romise Activities

...movement
...ryption
...shell deployment
...rrency mining

certego

Focus on initial access
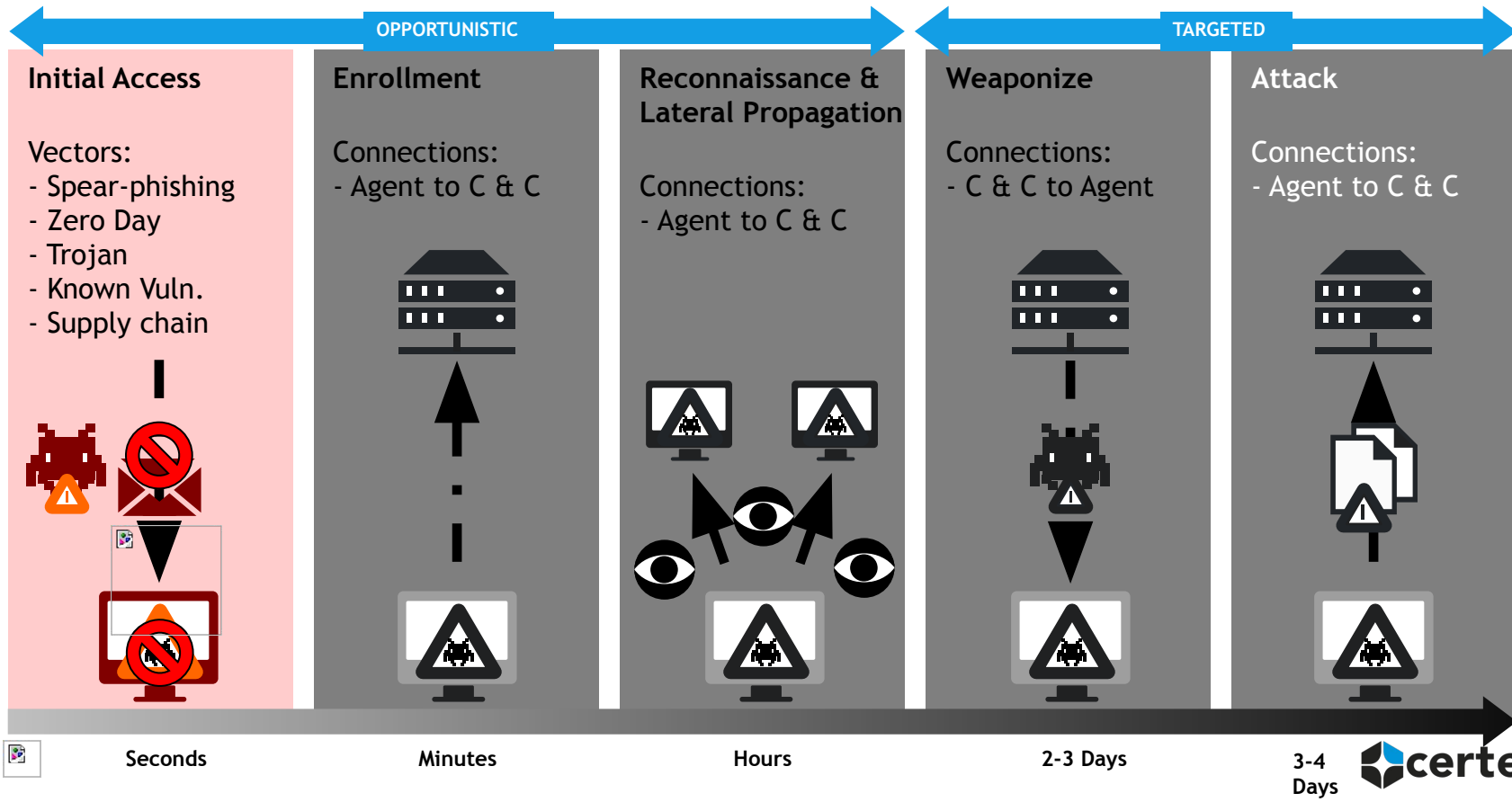
An Open source solution for the authentication protection of your organization

certego

BuffaLogs overview

Filebeat → Elasticsearch

query | read logins data

Detection engine

django

CELERY

Rabbit MQ

Database ↔ Web interface

NGINX
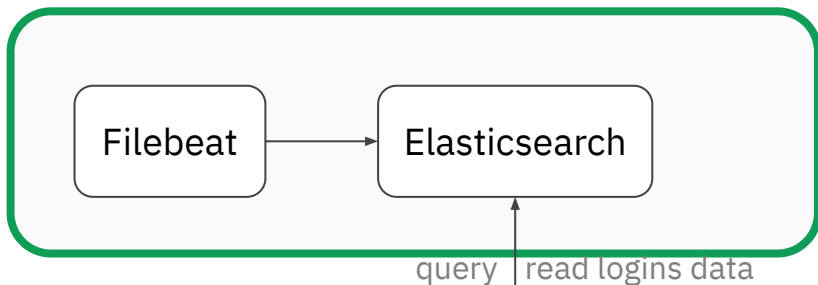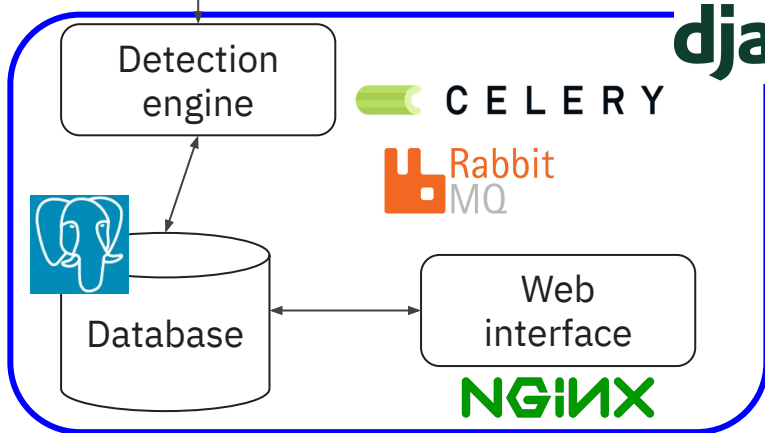
BuffaLogs

"bring your own database"
- Elasticsearch
- Splunk
- File
- etc.

certego

BuffaLogs architecture
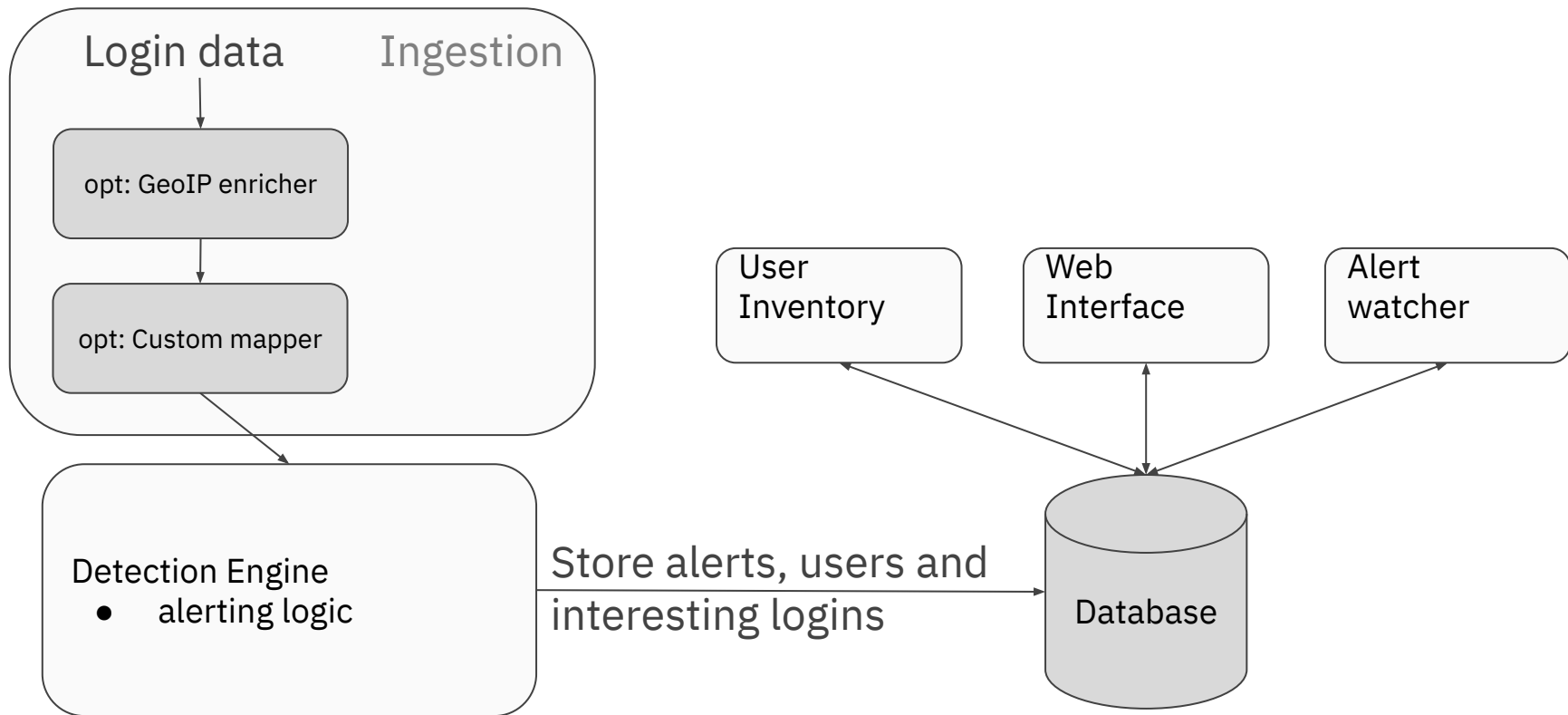
Installation & Setup

Docker containerized application
& Django Reusable App

1 Clone BuffaLogs locally:
> git clone git@github.com:certego/BuffaLogs.git

2 Run the application container:
> docker compose up -d buffalogs

3 Create django superuser
> docker exec -it buffalogs python3 manage.py
createsuperuser

4 Visualize django admin and homepage:
> localhost:8000/admin/
> localhost:8000/

certego

BuffaLogs web interface - v1

Users risk score analytics

Alerts geo map
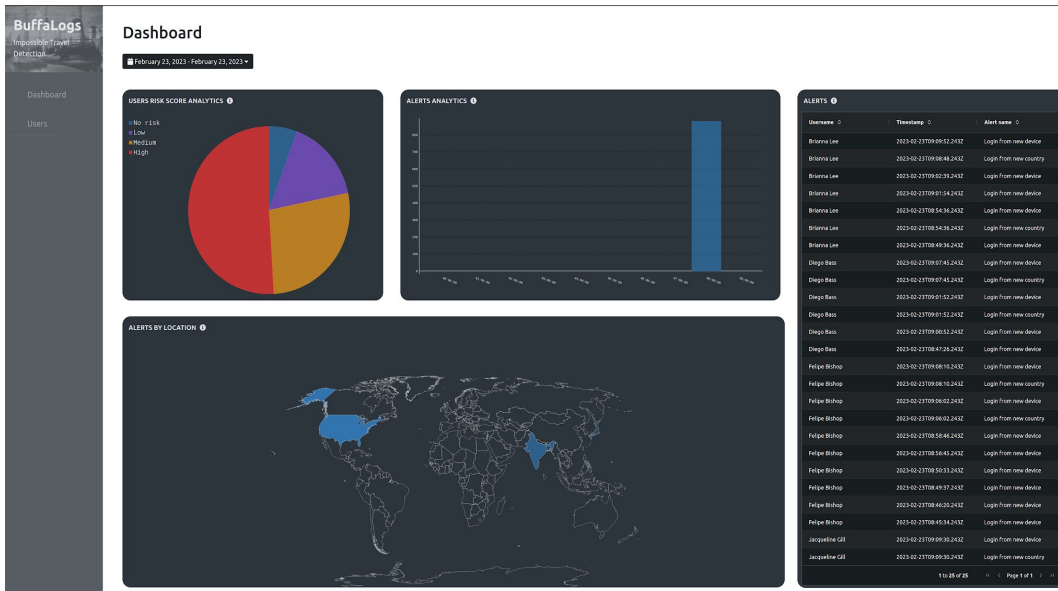
Alerts analytics period

Alerts list

certego

Detection types

- New Device
- New Country | Atypical country **WIP**
- Impossible Travel
- User Risk Threshold **WIP**
- Anonymous Ip Login **WIP**
- Stale account **WIP**

certego

Alerts types - example

Three login seen:
- 3:00 Milan
- 3:30 Rome

} 600 km / 0,5 h = 1200 km/h
→ Impossible travel

- 12:50 Vienna → New Country

  - ... 30 days later: Austria Login → Atypical Country

If <u>also</u>:
- with different user-agents → New Device
- with anonymous IPs → Anonymous IP Login

© Vemaps.com

certego

Alerts types - Stale accounts example

BuffaLogs can be configured to keep a list of users in a system (now supported: LDAP, Azure AD)

User name	Creation Date
o.bennett	10/01/2025
e.wright	20/01/2025
a.blackwood	29/01/2025
m.turner	09/06/2024
j.doe	10/12/2024

diff

User name	Last Login
o.bennett	10/01/2025
e.wright	27/01/2025
a.blackwood	29/01/2025
m.turner	20/07/2024

Alert Stale accounts:
- m.turner last login is more than 30 days ago
- j.doe is active but they never logged in

certego

Detection logic

Processing: normalization

Document

event.category: <mark>authentication</mark> @timestamp: Jan 7, 2025 @ 11:41:
agent.id: b0540b62-c53c-42a4-8b36-998bbcfa3283   agent.name: filel
azure.correlationId: 1dd9ea88-8bc7-4334-9cf8-bcc2b2427536   azure
azure.resourceId: ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
azure.service.application.displayName: Microsoft Teams   azure.se

event.category: <mark>authentication</mark> @timestamp: Jan 7, 2025 @ 11:41:
agent.id: b0540b62-c53c-42a4-8b36-998bbcfa3283   agent.name: filel
azure.correlationId: e2334398-00f3-41b7-8bda-e7bee66dc483   azure
azure.resourceId: ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
when the user was signing-in.   azure.result.signature: None   azure

event.category: <mark>authentication</mark> @timestamp: Jan 7, 2025 @ 11:41:
agent.id: b0540b62-c53c-42a4-8b36-998bbcfa3283   agent.name: filel
azure.correlationId: 3ce68113-ac9a-4795-9041-f7d796a45979   azure
azure.resourceId: ▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮▮
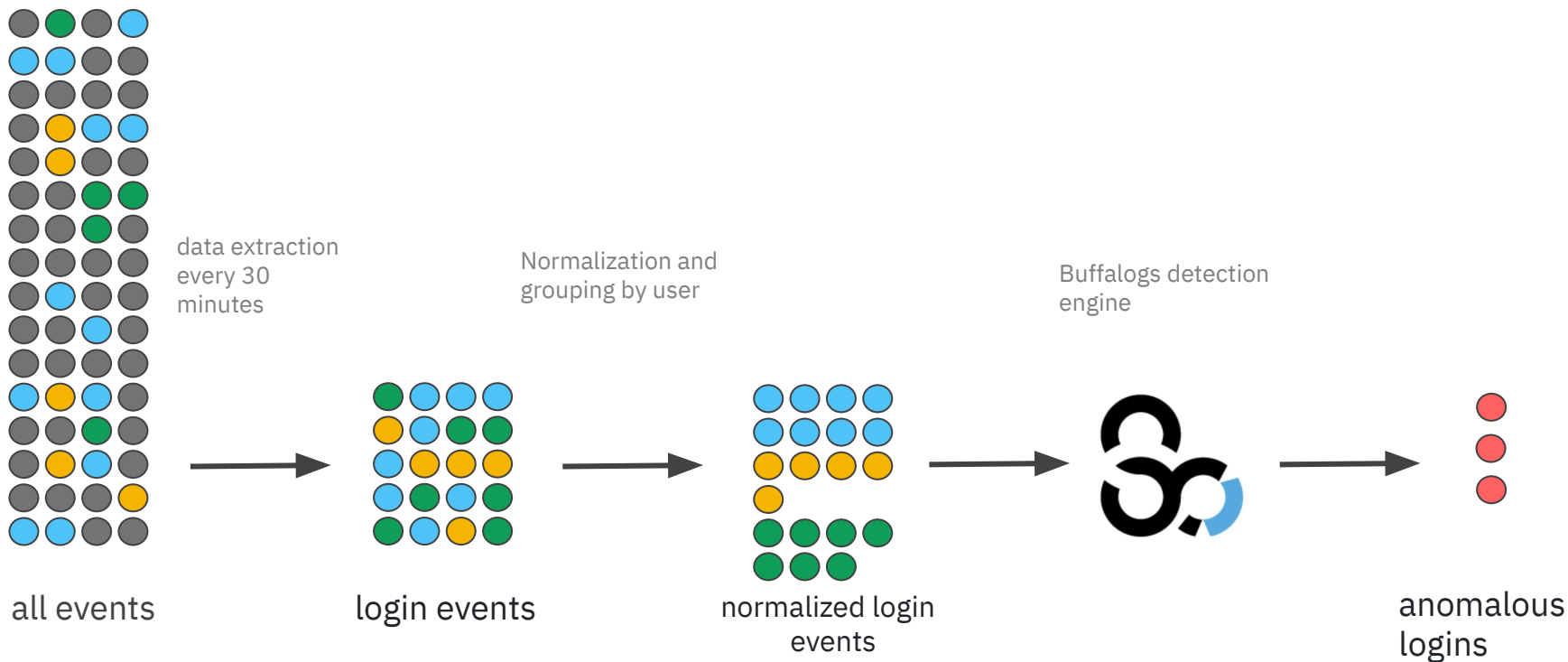azure.service.application.displayName: Microsoft App Access Pane

event.category: <mark>authentication</mark> @timestamp: Jan 7, 2025 @ 11:41:
agent.id: b0540b62-c53c-42a4-8b36-998bbcfa3283   agent.name: filel
azure.correlationId: 15ed6421-cf88-40fe-a7f7-7754cecd6a2d   azure

every
30 mins

"**timestamp**": "*<login_datetime>*",
"**index**": "*<log_source_index>*",
"**id**": "*<log_unique_id>*"
"**user**": {
    "**name**": "*<user_name>*"
  },
  "**source**": {
    "**geo**": {
      "**country_name**": "*<country_origin_log>*",
      "**location**": {
        "**lat**": "*<log_latitude>*",
        "**lon**": "*<log_longitude>*"
      }
    },
    "**as**": {
      "**organization**": {
        "**name**": "*<ISP_name>*"
      }
    },
    "**ip**": "*<log_source_ip>*"
  },
  "**user_agent**": {
    "**original**": "*<log_device_user_agent>*"
  },
"**event**": { "**type**": "**start**", "**category**": "**authentication**",
"**outcome**": "**success**"}}

Processing: collecting logins

data extraction every 30 minutes

Normalization and grouping by user

Buffalogs detection engine

all events

login events

normalized login events

anomalous logins

certego

What we have learned

We have deployed BuffaLogs in Certego detection platform:

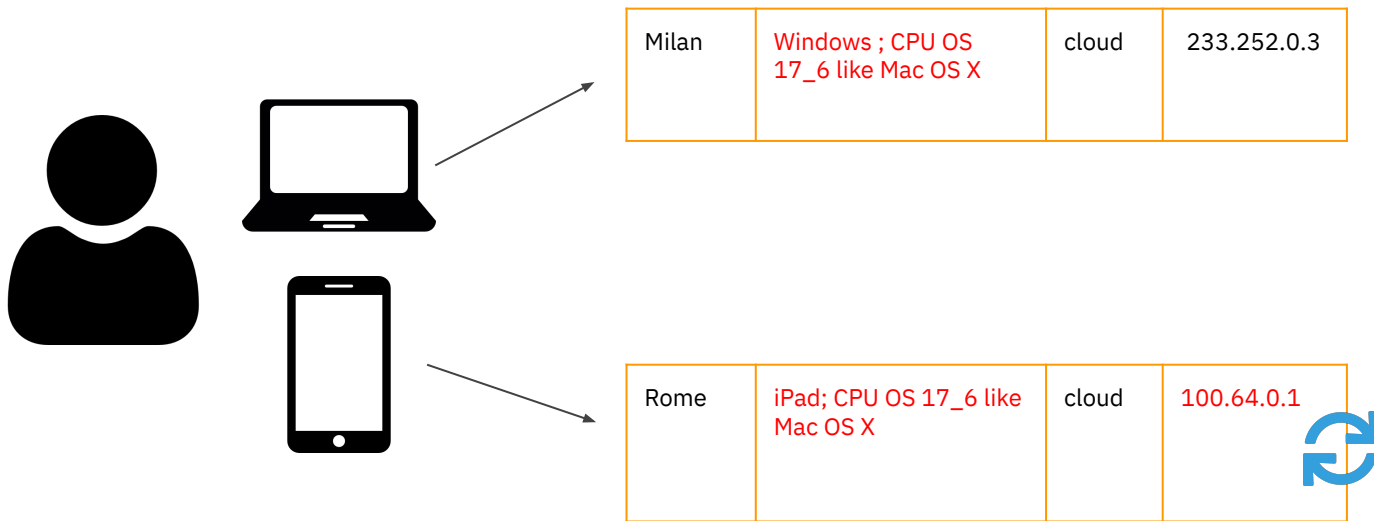- monitoring 300.000 logins each hour
- monitoring 30+ customers

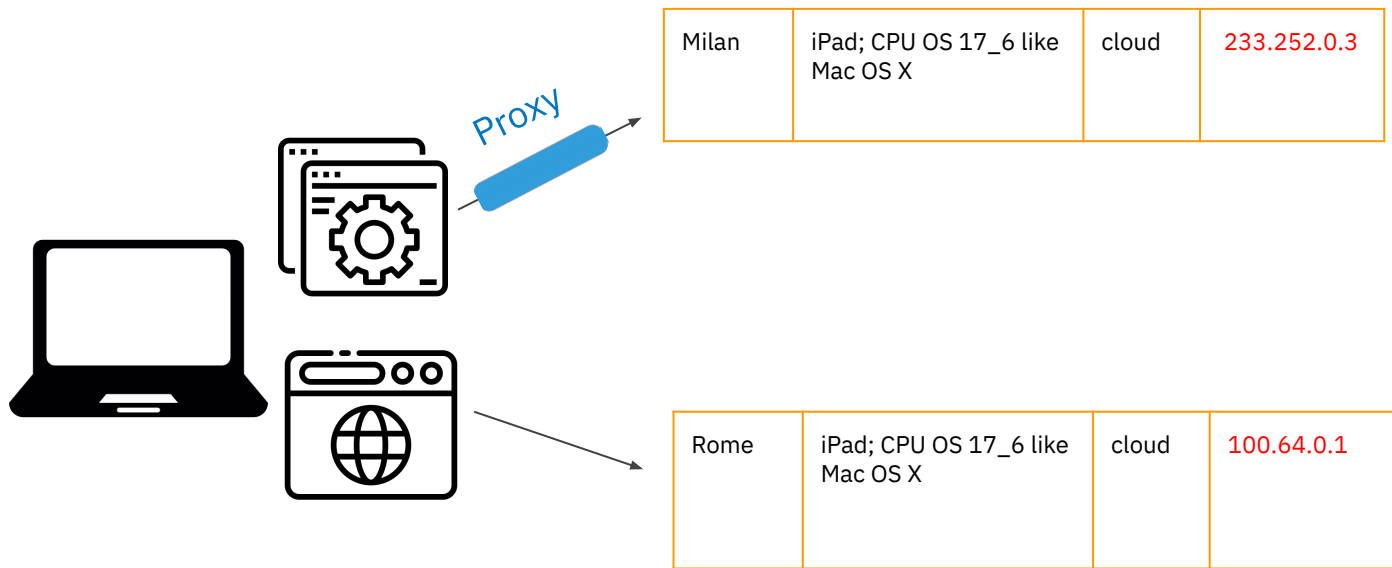Event logs collected from:

- Azure AD (Entra ID)
- VPN
- LDAP

certego

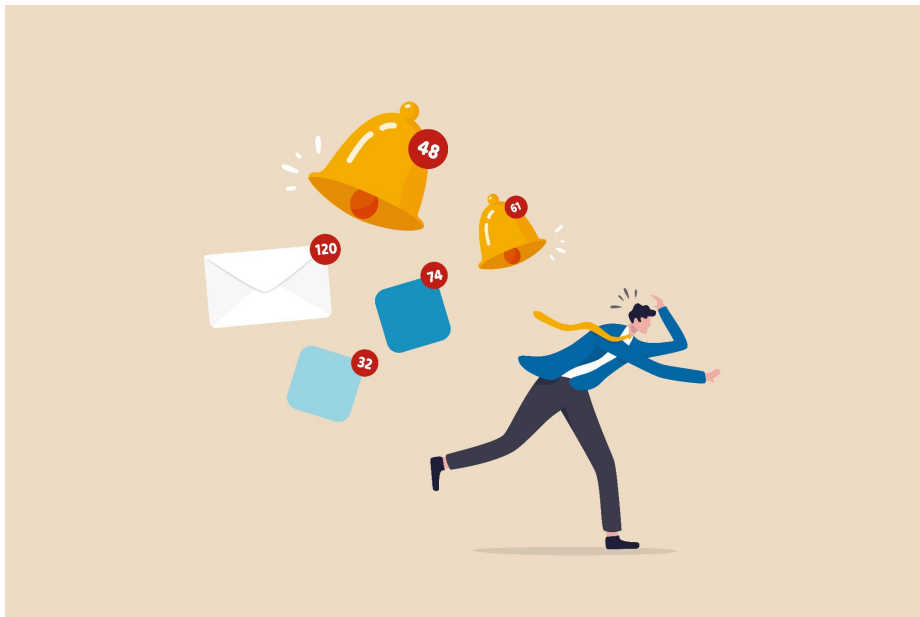# Critical aspects

certego

Smartphone/Computer - the aspect

Milan	Windows ; CPU OS 17_6 like Mac OS X	cloud	233.252.0.3

Rome	iPad; CPU OS 17_6 like Mac OS X	cloud	100.64.0.1

Proxied IPs - the aspect

Milan	iPad; CPU OS 17_6 like Mac OS X	cloud	233.252.0.3

Proxy

Rome	iPad; CPU OS 17_6 like Mac OS X	cloud	100.64.0.1

certego

Proxied IPs - the impact

Too many alerts

and... User profile creation (based on behaviors) was made impossible

TLP: WHITE

certego

Proxied IPs - the solution

Config model for custom filters:
- about **users**:
  - ignored/enabled users
  - vip users & alert is vip only
  - alert minimum *risk_score*
- about **location**:
  - ignored IPs
  - allowed countries
- about **devices**:
  - ignored ISPs
  - ignore mobile logins
- about **alerts**:
  - filtered alerts types

TLP: WHITE

Config object (1)

Detection filters - users

Ignored users:
`Not Available,N/A`
List of users (strings or regex patterns) to be ignored from the detection

Enabled users:
List of selected users (strings or regex patterns) on which the detection will perform

Vip users:
List of users considered more sensitive

☐ Alert is vip only
Flag to send alert only related to the users in the vip_users list

Alert minimum risk score: No risk ▾

Detection filters - location

Ignored ips:
List of IPs to remove from the detection

Allowed countries:
List of countries to exclude from the detection, because 'trusted' for the customer

Detection filters - devices

Ignored ISPs:
List of ISPs names to remove from the detection

☐ Ignore mobile logins
Flag to ignore mobile devices from the detection

Detection filters - alerts

Filtered alerts types:
Login from new device
Impossible Travel detected
Login from new country
User risk higher than threshold
Login from an anonymizer IP
Login from a country not visited recently

Proxied IPs - the solution

- impossible travel **metrics**:
  - distance & speed accepted for considering a trip "licit"
- clean models **metrics**:
  - users/logins/alert/ip max info expiration in days

→ sort of "bring your own detection"

certego

wrong Geolocation - the aspect

IP	IPGeolocation.io	Maxmind's GeoLite2 Database	IP2Location Lite	ip2c.org	GeoIP Nekudo	IP API
xxx.180.170.246	Rome, Italy	Reggio Emilia, Italy	Modena (MO), Italy	Italy	Fidenza, Italy	Bomporto, Italy
xxx.161.229.3	Berlin, Germany	Bruxelles, Belgium	Bruxelles, Belgium	Germany	Frankfurt am Main, Germany	Bruxelles, Belgium

- the impact - wrong login locations
- the solution - on our event data, MaxMind has proven to be the most effective geolocation service
  - You should try out different geolocation provider and see what fit best your data

certego

BuffaLogs future plan

- Adding additional log sources
- Adding active alert notifications
- Adding users sync features
- **Automatic user blocking**
  - When a risk level of a user becomes too high, the system blocks the user automatically
- AI/ML/LLM (really?)

certego

BuffaLogs and Google Summer of Code

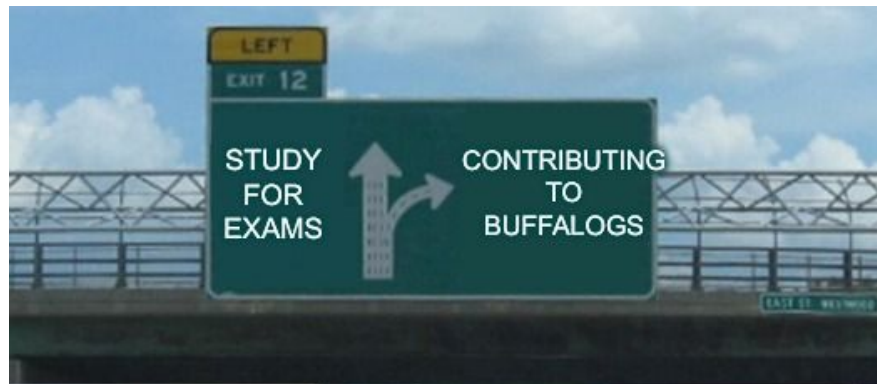Since the very beginning of this project we participated in the Google Summer of Code.

Google Summer of Code

We are looking for enthusiastic new contributors!

Please check our repo for updates:

https://github.com/certego/BuffaLogs

certego

Thank you!

via F. Lamborghini, 81 (MO) – Italy
T: +39 059 7353333
info@certego.net
www.certego.net