POLITÉCNICO DE LEIRIA

Security in SmartEmotion Platform

Carla Mendes - 2220663
Carlos Costa – 2220662
Rafael Pereira - 2220659

Tabela de Conteúdos

1 Introdução

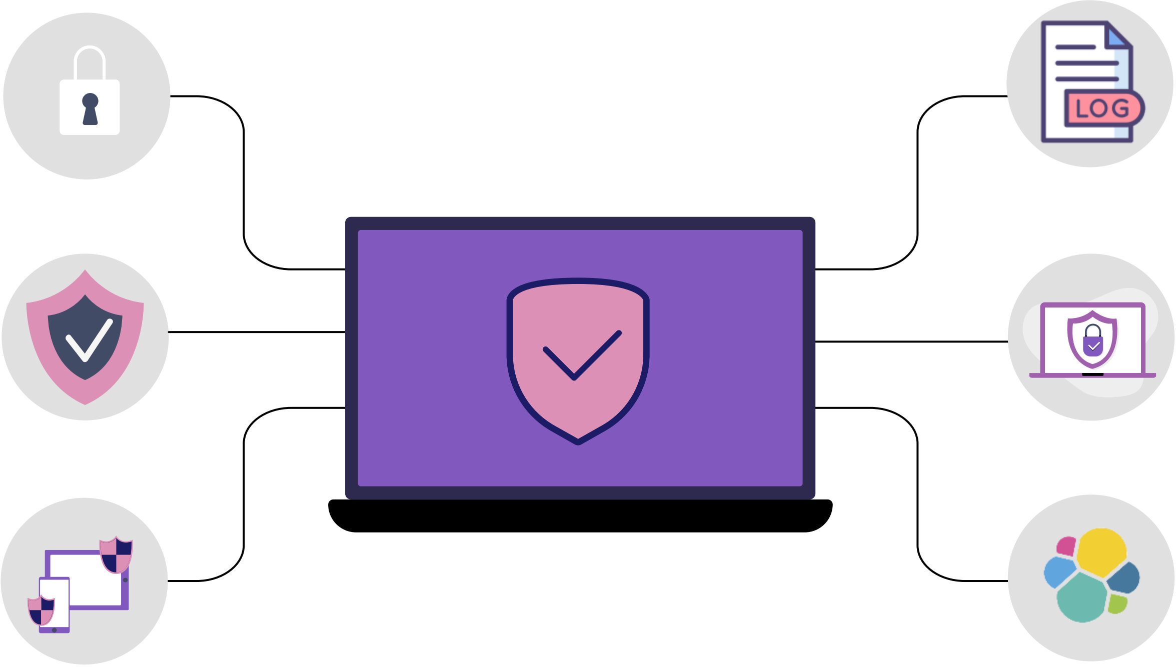
2 Background

3 Plataforma

4 Proposta de Solução

5 Conclusão

1. Introdução



Dados e Informações
Recursos importantes para qualquer negócio

Segurança
Ponto crucial em qualquer sistema

SmartEmotion
Solução implementada

Ficheiros *Logs*
Análise e comparação

SIEM
Security Information and Event Management

Elastic
Soluções de busca simplificadas

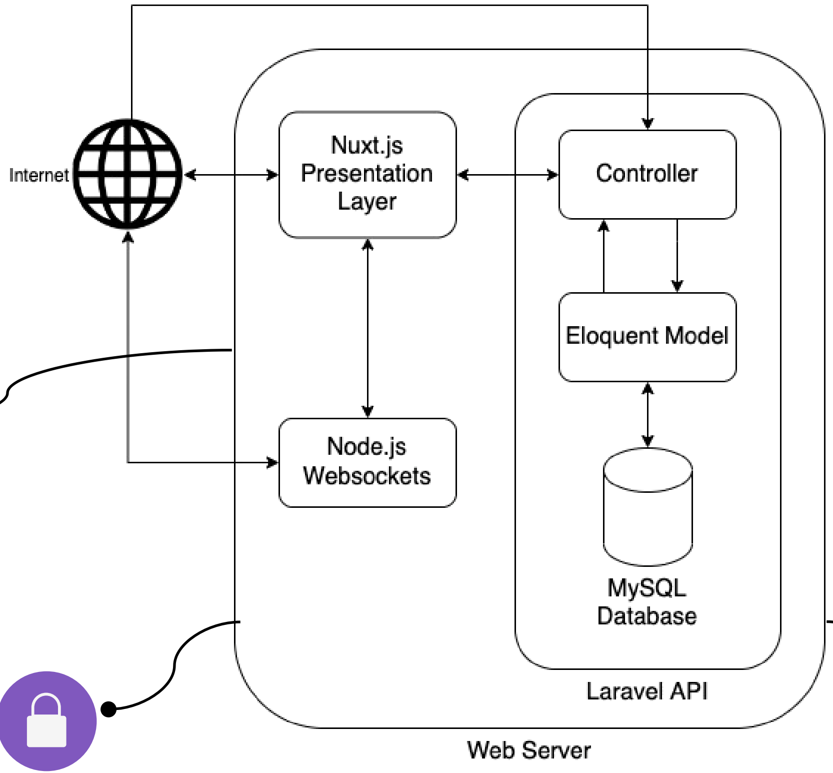
2. Background

- PII
- Ficheiros *Logs*
- SIEM
- Ataques cibersegurança

3. Plataforma - SmartEmotion

Idosos	Acompanhamento remotamente e em tempo real
Serviço Elder Home	Acompanhamento do estado emocional dos idosos
Plataforma	Alertar o estado emocional do idoso
Componentes	*Website*, API, base de dados, protocolo de comunicação assíncrona

3. Plataforma - Arquitetura

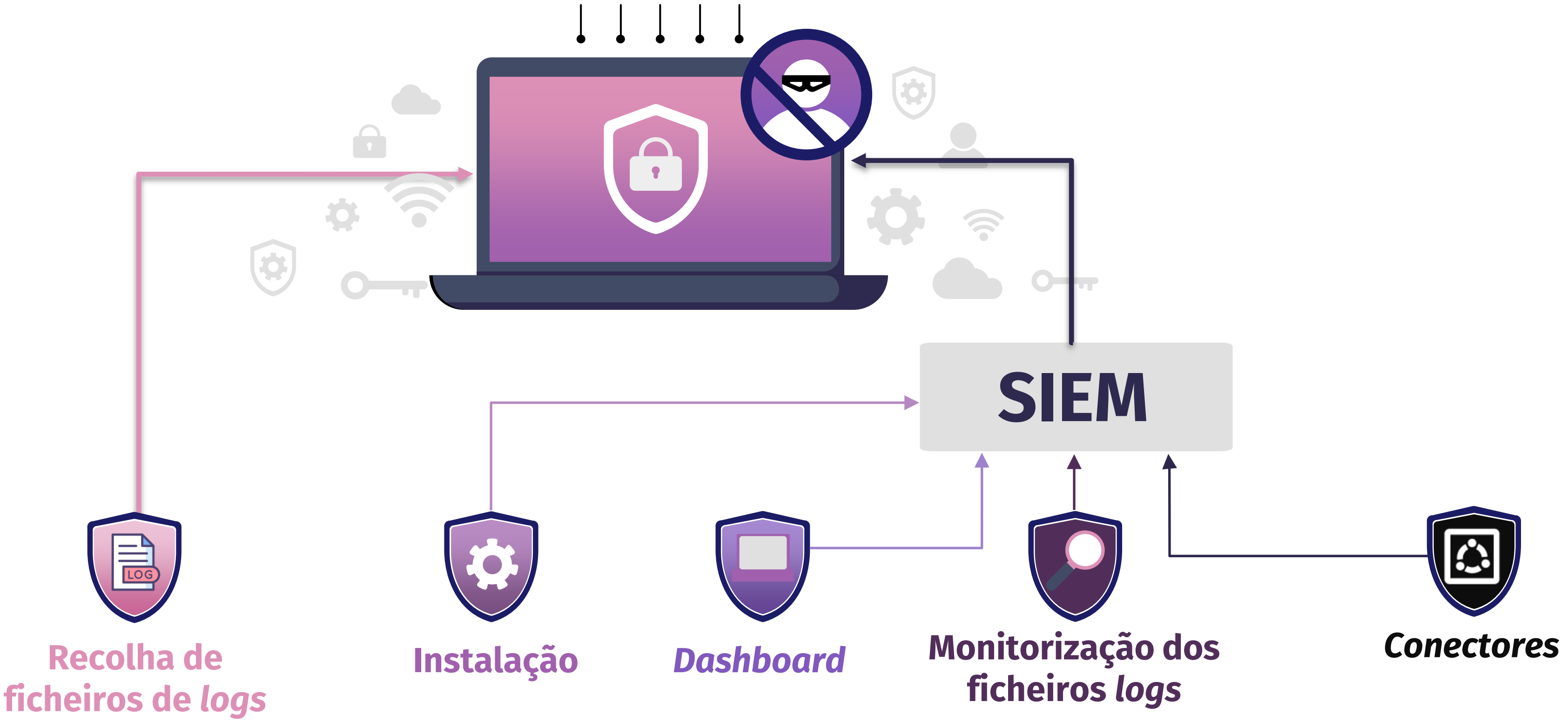


Disponível em qualquer lugar e qualquer tempo

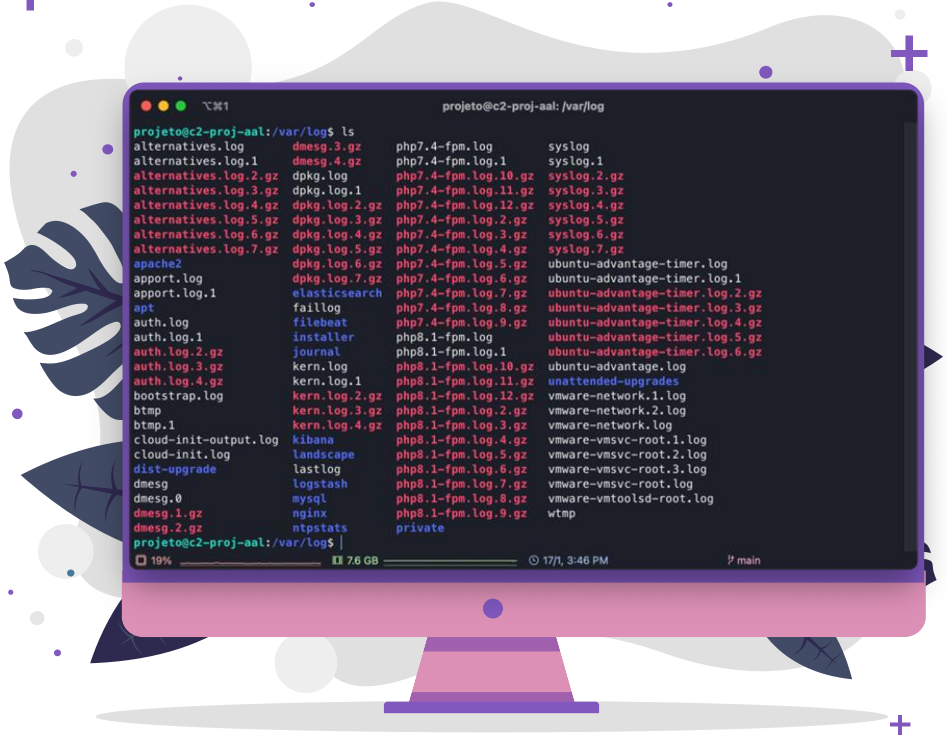
Assegurar a segurança em vários níveis

Reverse Proxy

4. Proposta de Solução


SIEM
LOG
Recolha de ficheiros de *logs*
Instalação
Dashboard
Monitorização dos ficheiros *logs*
Conectores

4.1 Ficheiros Logs



```
projeto@c2-proj-aal:/var/log$ ls
alternatives.log       dmesg.3.gz     php7.4-fpm.log        syslog
alternatives.log.1     dmesg.4.gz     php7.4-fpm.log.1      syslog.1
alternatives.log.2.gz  dpkg.log       php7.4-fpm.log.10.gz  syslog.2.gz
alternatives.log.3.gz  dpkg.log.1     php7.4-fpm.log.11.gz  syslog.3.gz
alternatives.log.4.gz  dpkg.log.2.gz  php7.4-fpm.log.12.gz  syslog.4.gz
alternatives.log.5.gz  dpkg.log.3.gz  php7.4-fpm.log.2.gz   syslog.5.gz
alternatives.log.6.gz  dpkg.log.4.gz  php7.4-fpm.log.3.gz   syslog.6.gz
alternatives.log.7.gz  dpkg.log.5.gz  php7.4-fpm.log.4.gz   syslog.7.gz
apache2                dpkg.log.6.gz  php7.4-fpm.log.5.gz   ubuntu-advantage-timer.log
apport.log             dpkg.log.7.gz  php7.4-fpm.log.6.gz   ubuntu-advantage-timer.log.1
apport.log.1           elasticsearch  php7.4-fpm.log.7.gz   ubuntu-advantage-timer.log.2.gz
apt                    faillog        php7.4-fpm.log.8.gz   ubuntu-advantage-timer.log.3.gz
auth.log               filebeat       php7.4-fpm.log.9.gz   ubuntu-advantage-timer.log.4.gz
auth.log.1             installer      php8.1-fpm.log        ubuntu-advantage-timer.log.5.gz
auth.log.2.gz          journal        php8.1-fpm.log.1      ubuntu-advantage-timer.log.6.gz
auth.log.3.gz          kern.log       php8.1-fpm.log.10.gz  ubuntu-advantage.log
auth.log.4.gz          kern.log.1     php8.1-fpm.log.11.gz  unattended-upgrades
bootstrap.log          kern.log.2.gz  php8.1-fpm.log.12.gz  vmware-network.1.log
btmp                   kern.log.3.gz  php8.1-fpm.log.2.gz   vmware-network.2.log
btmp.1                 kern.log.4.gz  php8.1-fpm.log.3.gz   vmware-network.log
cloud-init-output.log  kibana         php8.1-fpm.log.4.gz   vmware-vmsvc-root.1.log
cloud-init.log         landscape      php8.1-fpm.log.5.gz   vmware-vmsvc-root.2.log
dist-upgrade           lastlog        php8.1-fpm.log.6.gz   vmware-vmsvc-root.3.log
dmesg                  logstash       php8.1-fpm.log.7.gz   vmware-vmsvc-root.log
dmesg.0                mysql          php8.1-fpm.log.8.gz   vmware-vmtoolsd-root.log
dmesg.1.gz             nginx          php8.1-fpm.log.9.gz   wtmp
dmesg.2.gz             ntpstats       private
projeto@c2-proj-aal:/var/log$ |
```

Análise

Análise de vulnerabilidades

Ficheiros logs

Auth, syslog, nginx, MySQL, logs customizados

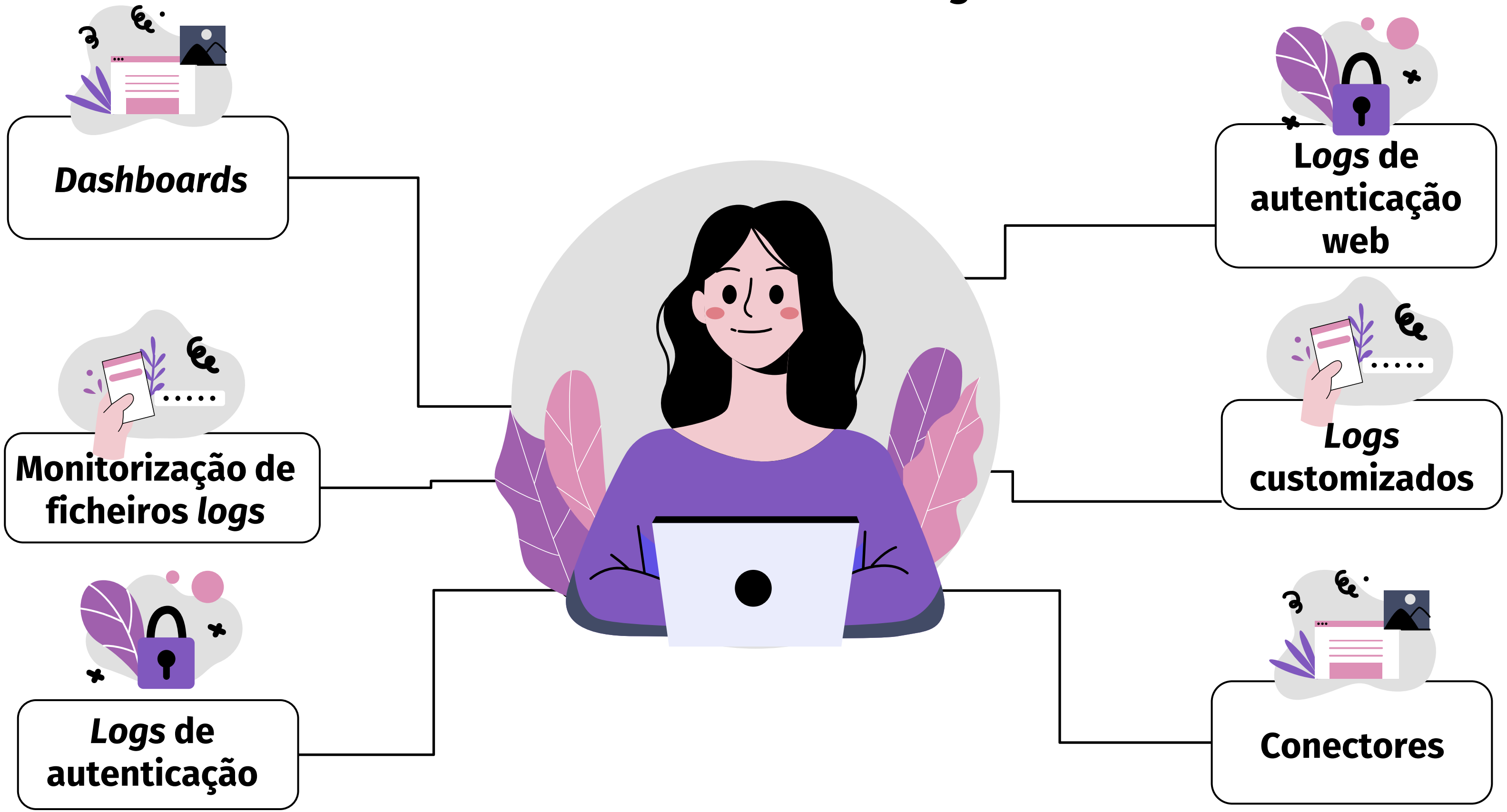
Ubuntu

Pasta logs: "/var/logs"

Container

Cópia da base de dados da plataforma SmartEmotion

4.2 Demonstração



Dashboards

Monitorização de ficheiros *logs*

Logs de autenticação

Logs de autenticação web

Logs customizados

Conectores

5. Conclusão

Segurança

SmartEmotion

Solução para acompanhar os idosos

Mecanismos de monitorização

Ficheiros *logs* e SIEM

Simulação de Ataques

Referências

- Elastic: https://www.elastic.co/pt/;
- Elastic Tutorial (Fosstechinx): https://www.fosstechnix.com/install-elastic-stack-on-ubuntu-20-04-lts/;
- Filebeat: https://www.elastic.co/guide/en/beats/filebeat/current/filebeat-overview.html;
- Kibana: https://www.elastic.co/guide/en/kibana/current/introduction.html;
- Logstash: https://www.elastic.co/guide/en/logstash/current/introduction.html;
- Elasticsearch: https://www.elastic.co/guide/en/elasticsearch/reference/current/elasticsearch-intro.html;
- Docker Logs: https://docs.docker.com/engine/reference/commandline/logs/;
- SIEMs: https://www.comparitech.com/net-admin/open-source-siem-tools/;
- PII: https://techbeacon.com/security/how-meet-privacy-requirements-your-pii;
- ELK Stack: https://www.elastic.co/what-is/elk-stack;
- Grok: https://logz.io/blog/logstash-grok/;
- Ubuntu: https://sematext.com/blog/ubuntu-logs/;
- Slidesgo: https://slidesgo.com/;
- Ubuntu: https://www.xilinx.com/products/design-tools/embedded-software/ubuntu.html;
- Flaticon: https://www.flaticon.com/.

Obrigado

Alguma questão?

Carla Mendes 2220663@my.ipleiria.pt
Carlos Costa 2220662@my.ipleiria.pt
Rafael Pereira 2220659@my.ipleiria.pt