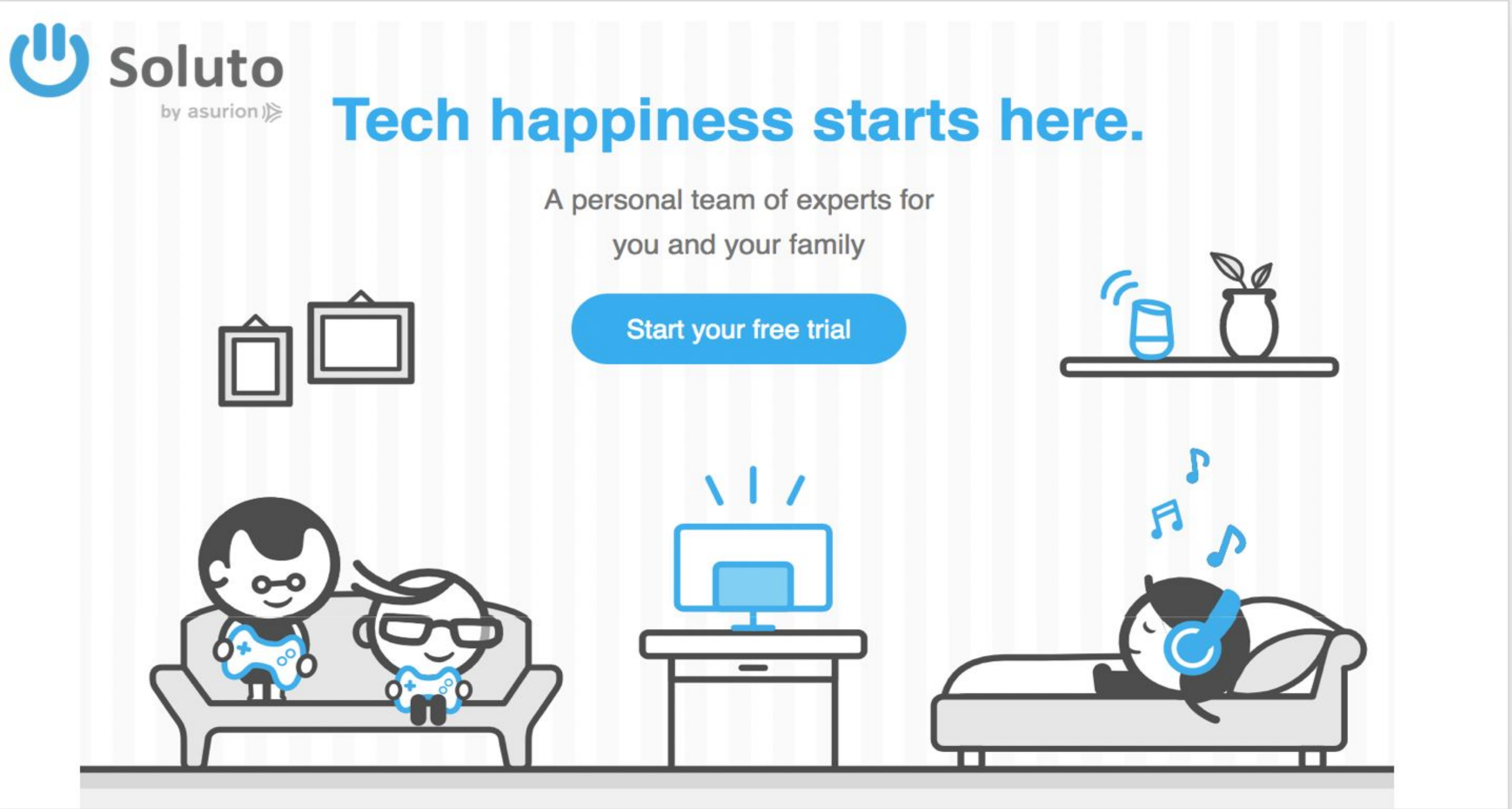
Soluto

icinga

Monitoria -
A Monitoring Democracy

@yaronidan

@SolutoEng



Soluto
by asurion

Tech happiness starts here.

A personal team of experts for
you and your family

Let’s think about it

Should we monitor everything?

Let’s think about it

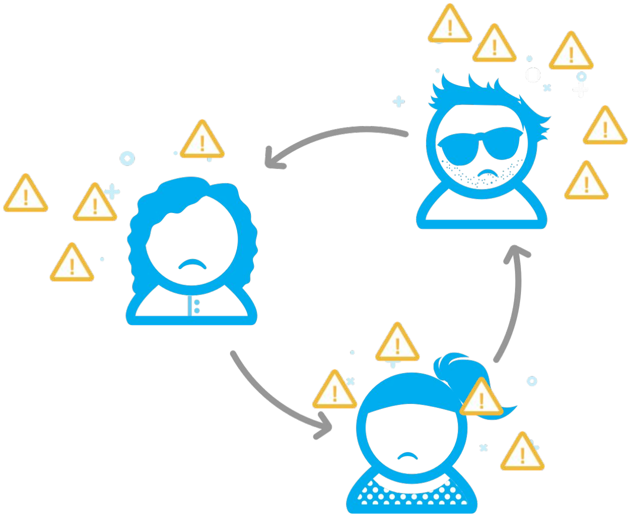
Can alerts suck less?

Let’s think about it

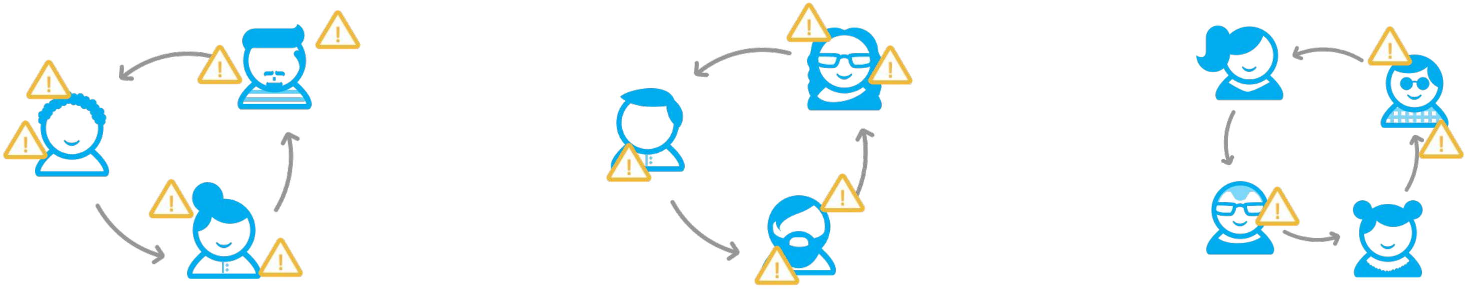
Who carries the pager?

One person

Rotating on-call duty



Rotating on-call duty per team

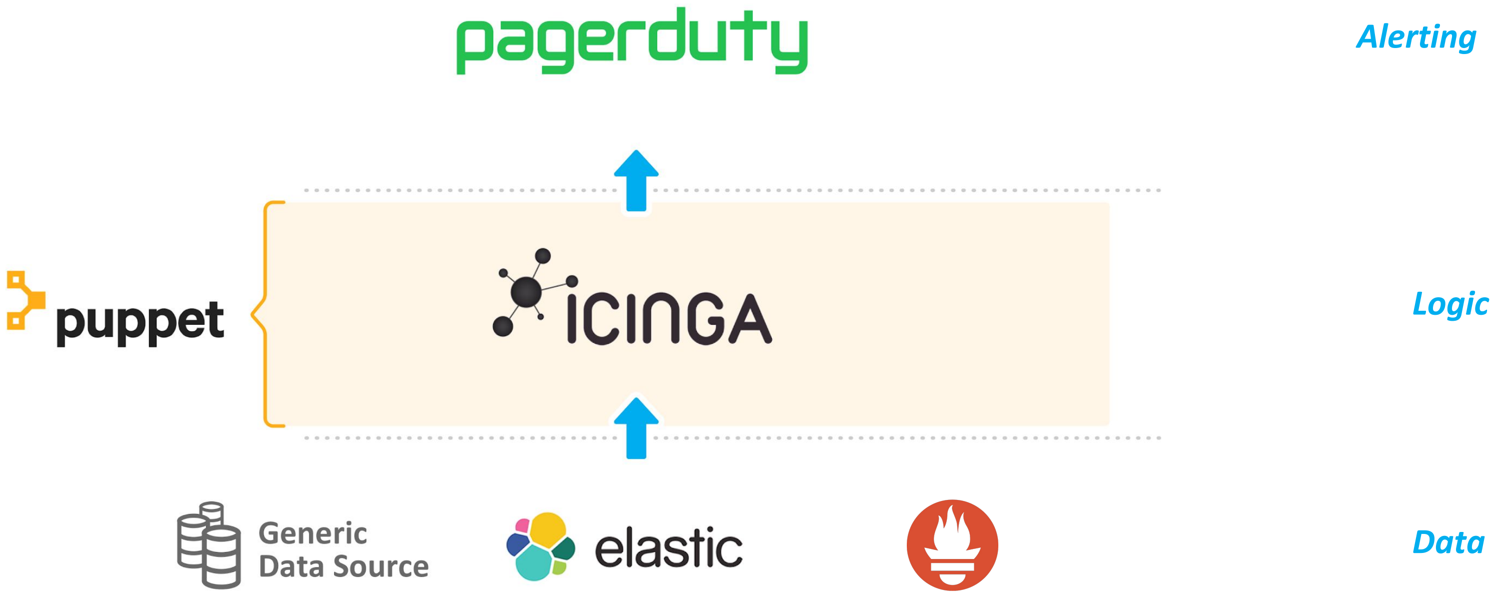


Cultural Shift

- *Culture was changing rapidly*
- *Developers needed a toolchain to enable this culture*

Technology Enables Culture

- *Self service*
- *Scalable*
- *Open source with a wide community*


pagerduty
Alerting
puppet
ICINGA
Logic
Generic
Data Source
elastic
Data

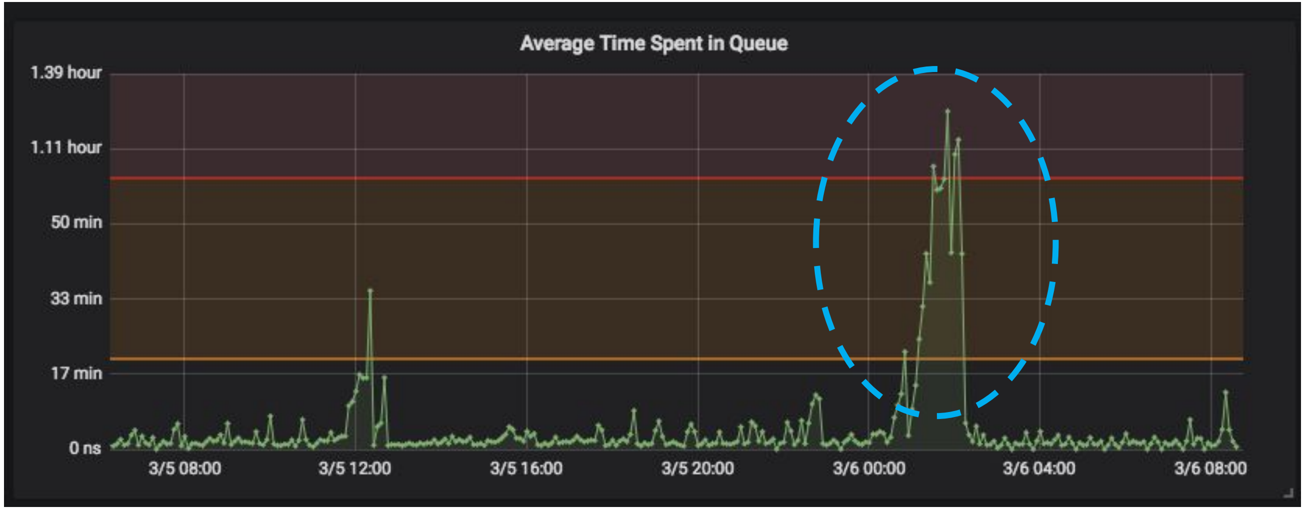
Generic
Data Source

elastic

Data

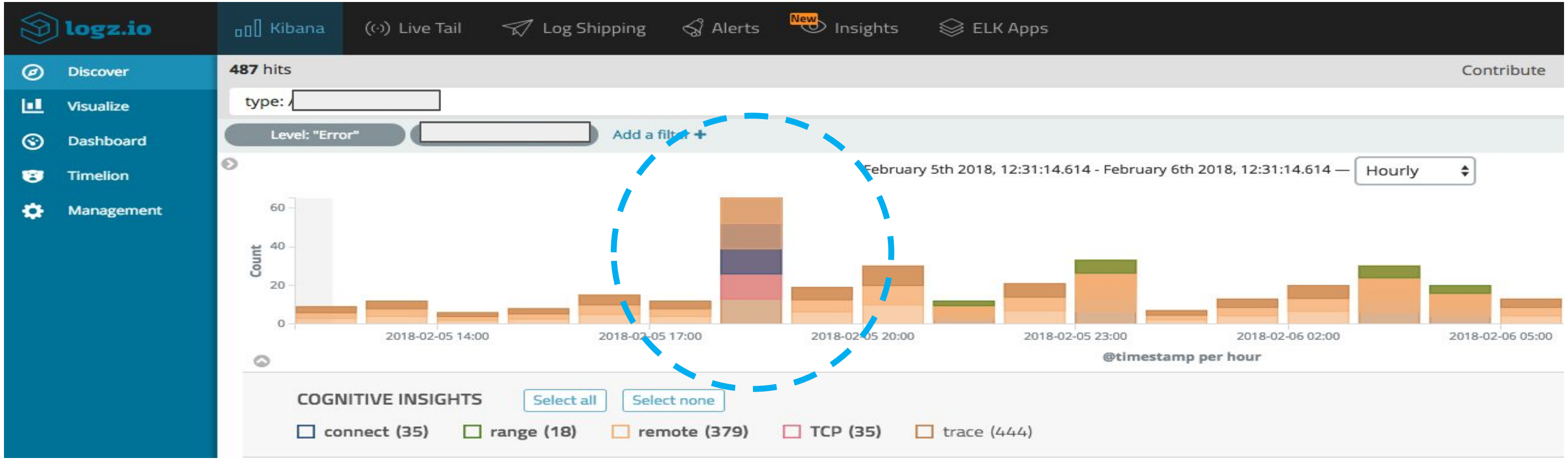
Where do we keep our monitoring data?

- *Metrics – Prometheus*



Where do we keep our monitoring data?

- *Metrics – Prometheus*
- *Logs - Elasticsearch*



487 hits

type: /[redacted]

Level: "Error" [redacted]

February 5th 2018, 12:31:14.614 - February 6th 2018, 12:31:14.614 — Hourly

COGNITIVE INSIGHTS

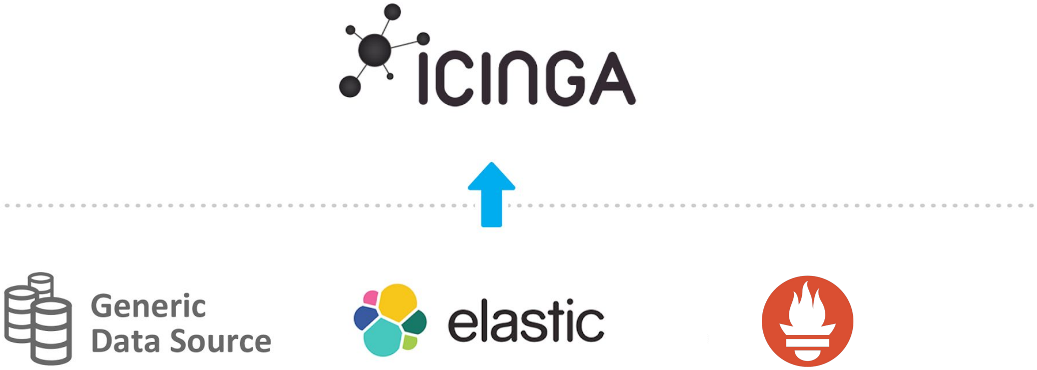
□ connect (35) □ range (18) □ remote (379) □ TCP (35) □ trace (444)

Where do we keep our monitoring data?

- *Metrics – Prometheus*
- *Logs - Elasticsearch*
- *Any other data source*

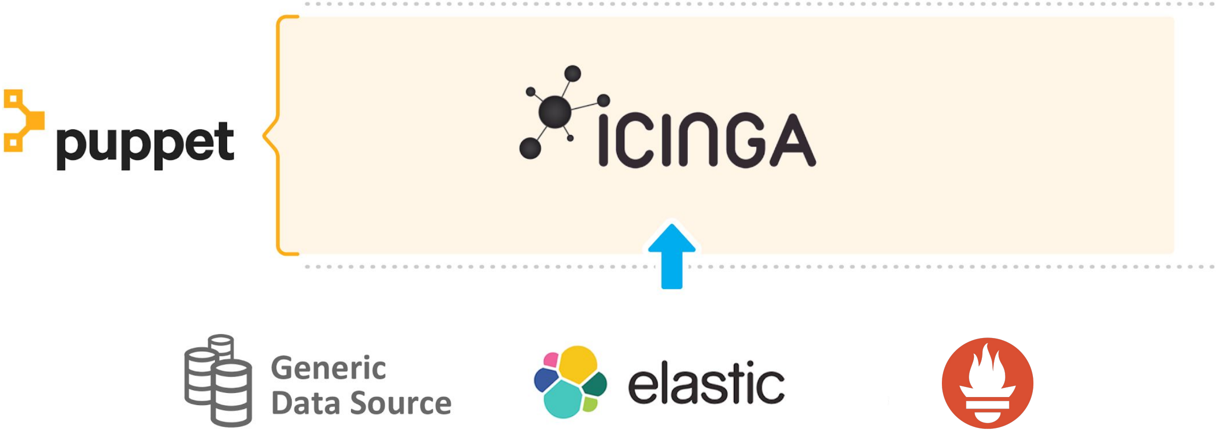
elastic

Generic
Data Source



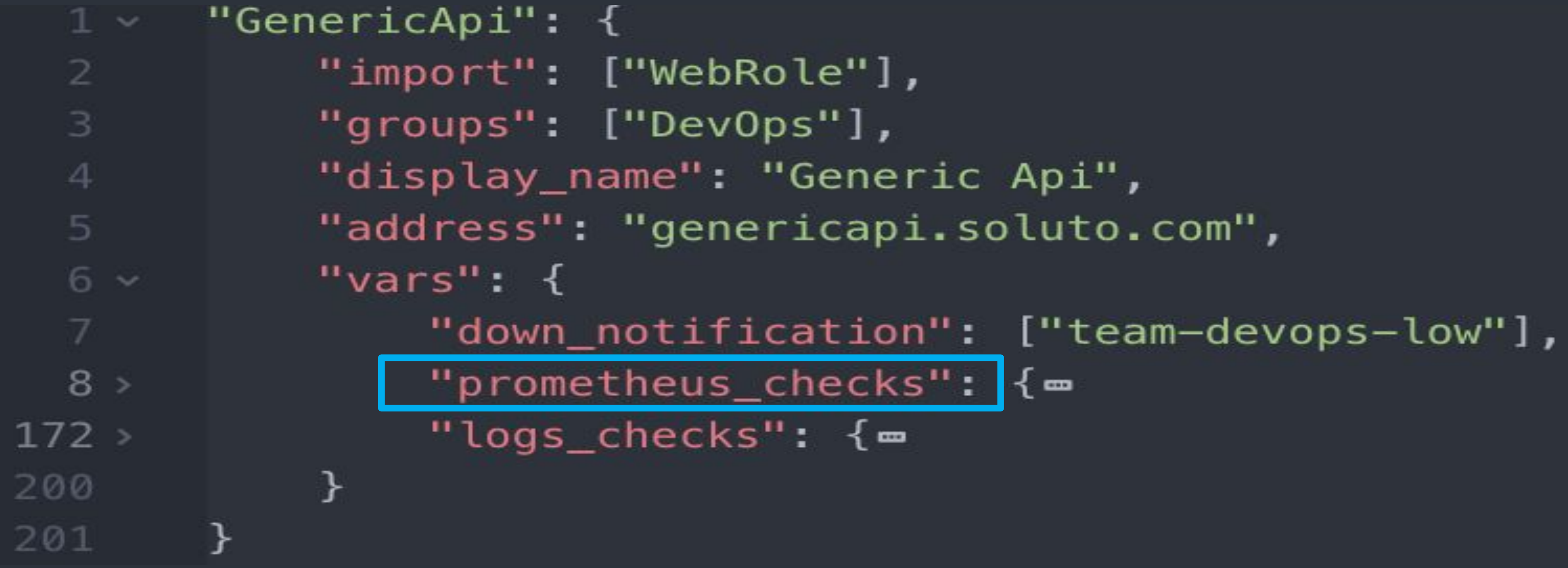
Logic

Data

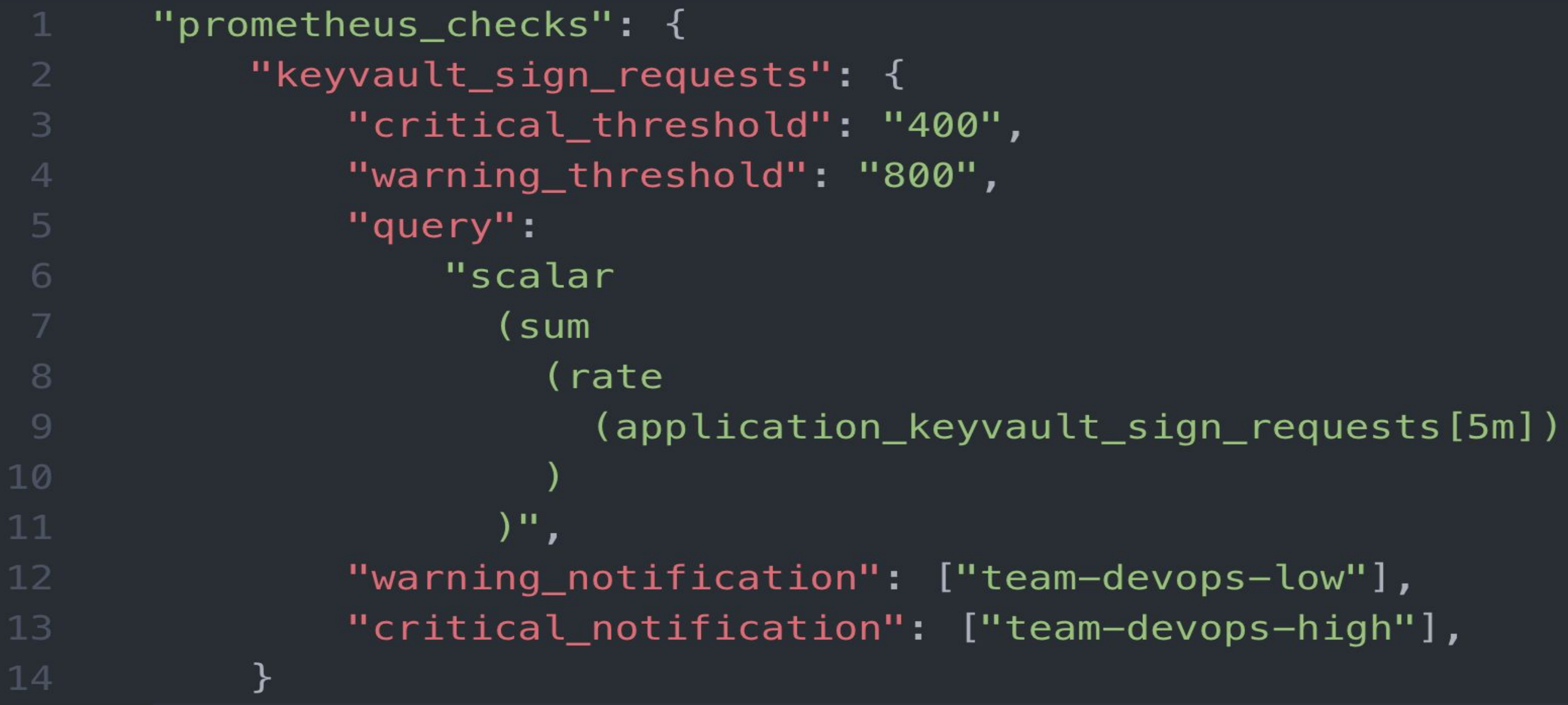


Logic

Data



```
"GenericApi": {
    "import": ["WebRole"],
    "groups": ["DevOps"],
    "display_name": "Generic Api",
    "address": "genericapi.soluto.com",
    "vars": {
        "down_notification": ["team-devops-low"],
        "prometheus_checks": {⋯
        "logs_checks": {⋯
    }
}
```



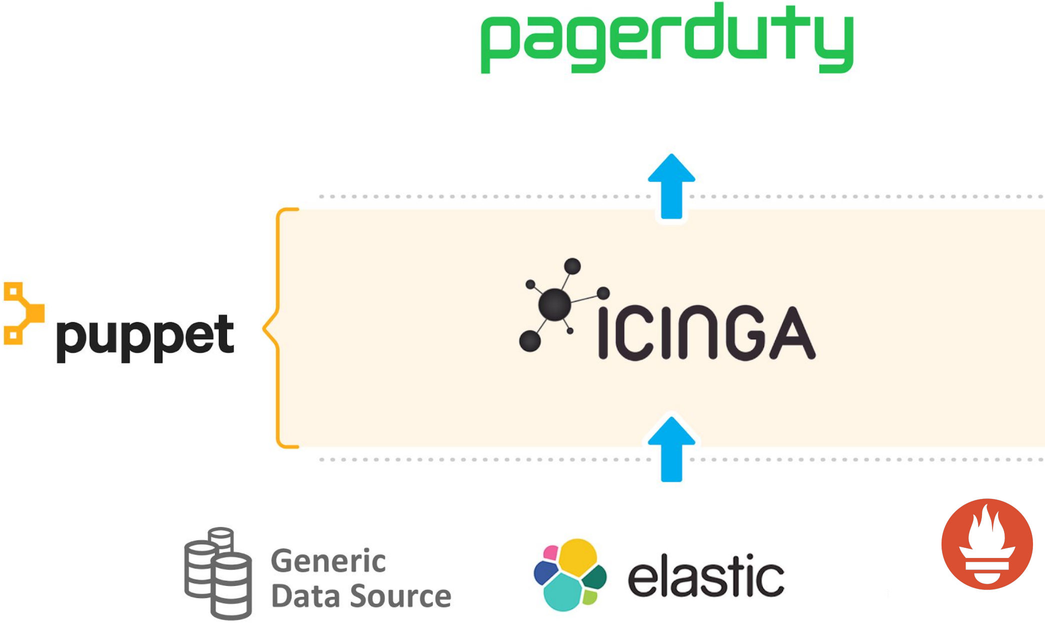
```
"prometheus_checks": {
    "keyvault_sign_requests": {
        "critical_threshold": "400",
        "warning_threshold": "800",
        "query":
            "scalar
              (sum
                (rate
                  (application_keyvault_sign_requests[5m])
                )
              )",
        "warning_notification": ["team-devops-low"],
        "critical_notification": ["team-devops-high"],
    }
```

Let’s take a look at the engine...

- *Monitoring-as-code*
- *Modular*
- *We can monitor anything we can think of*

ICINGA

puppet



Alerting

Logic

Data

pagerduty

Did we accomplish what we set out to achieve?

Did we accomplish what we set out to achieve?

- ☑ *Self service*
- ☑ *Scalable*
- ☑ *Open source with a wide community*

Everybody contributes

(commit statistics for production Apr 7, 2016 - Mar 10, 2019)

6341 *commits in* **1071** *days*

Everybody contributes

(commit statistics for production Apr 7, 2016 - Mar 10, 2019)

6341 *commits in* **1071** *days*

5.6 commits per day

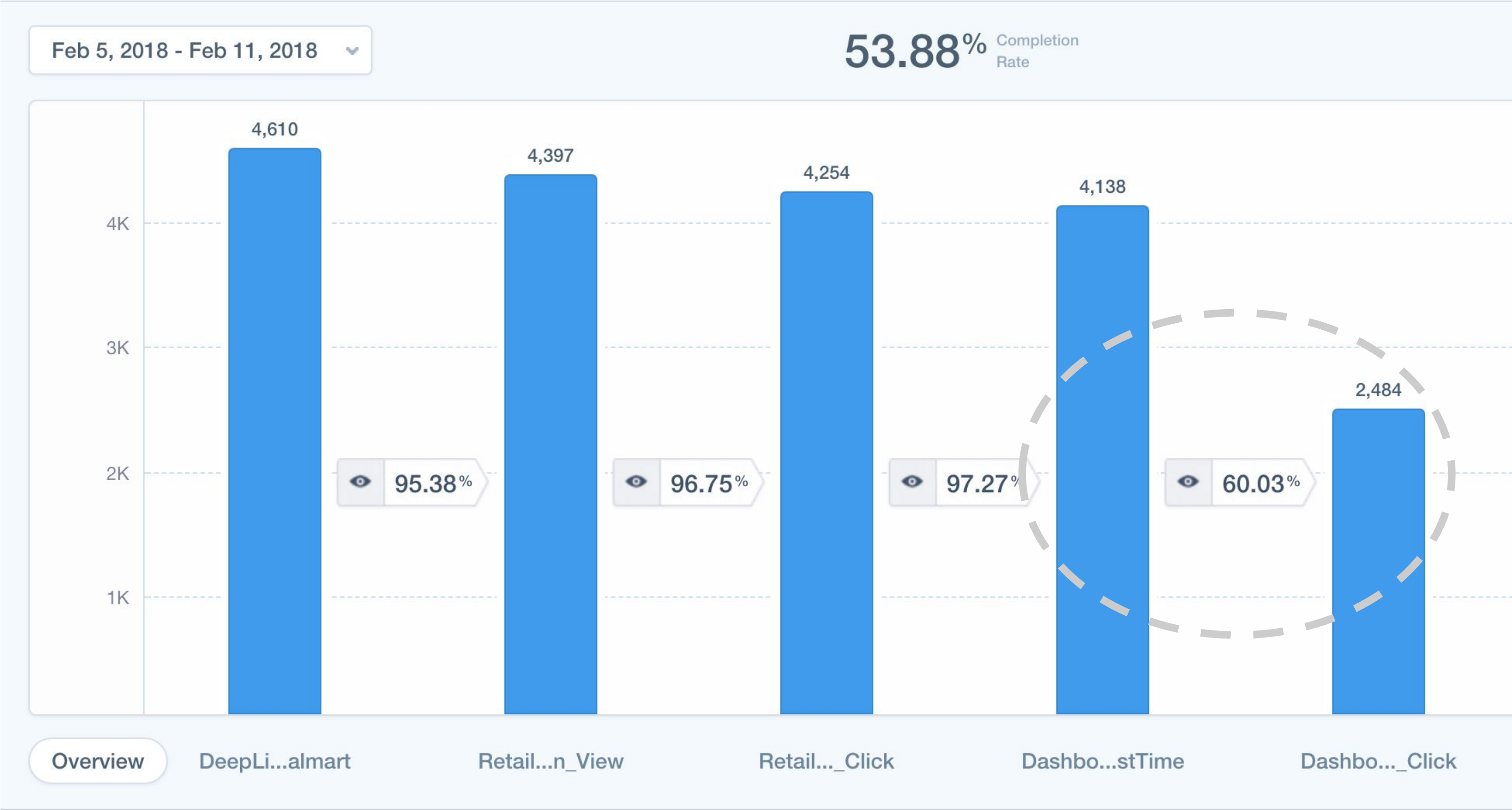
Everybody contributes

(commit statistics for production Apr 7, 2016 - Mar 10, 2019)

6341 *commits in* **1071** *days*

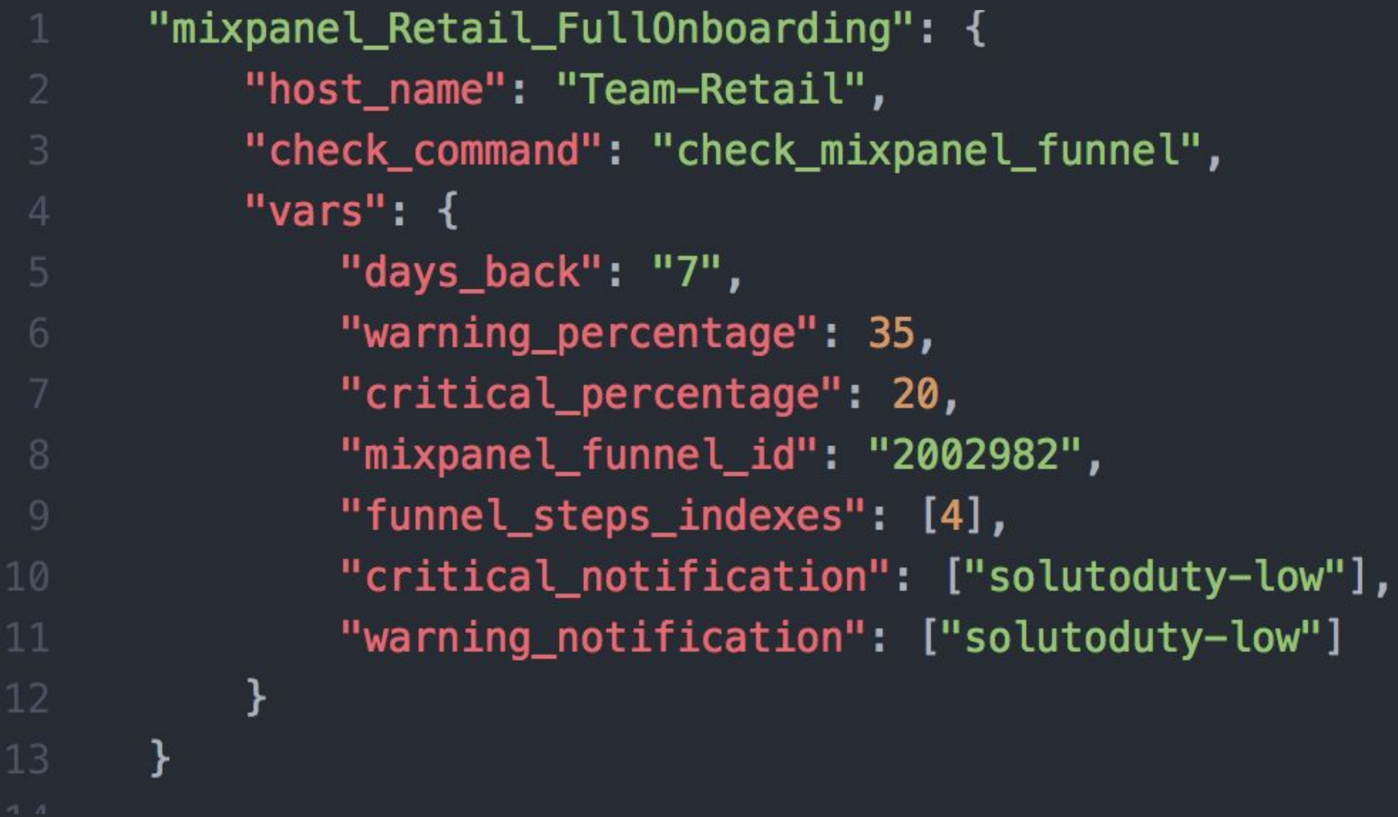
5.6 commits per day

Contributed by **75** *authors*



Feb 5, 2018 - Feb 11, 2018

53.88% Completion Rate



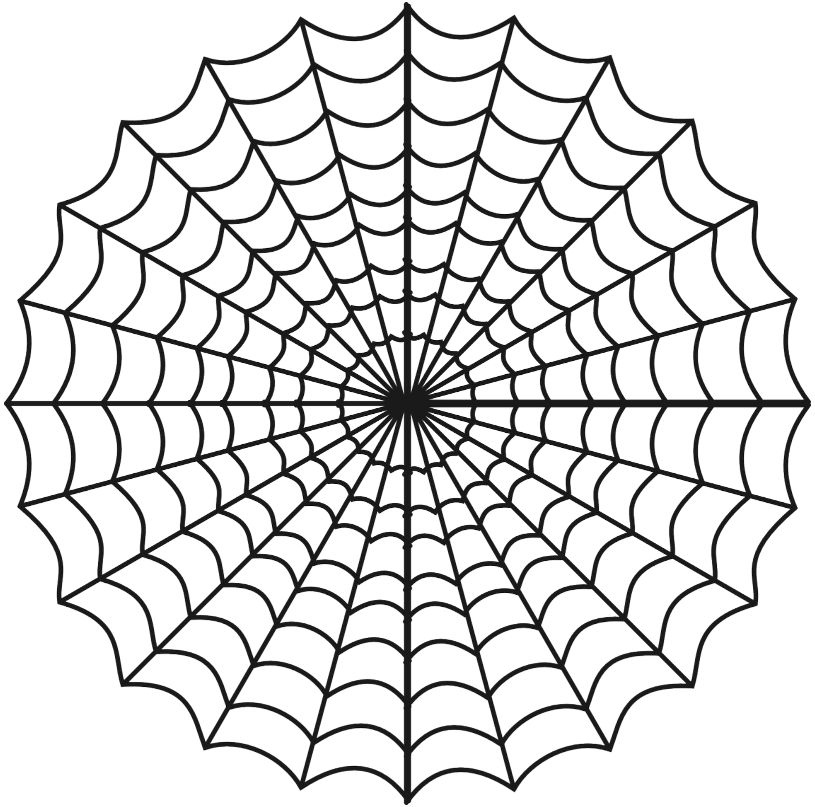
```
"mixpanel_Retail_FullOnboarding": {
    "host_name": "Team-Retail",
    "check_command": "check_mixpanel_funnel",
    "vars": {
        "days_back": "7",
        "warning_percentage": 35,
        "critical_percentage": 20,
        "mixpanel_funnel_id": "2002982",
        "funnel_steps_indexes": [4],
        "critical_notification": ["solutoduty-low"],
        "warning_notification": ["solutoduty-low"]
    }
}
```

Creating a Paved Road

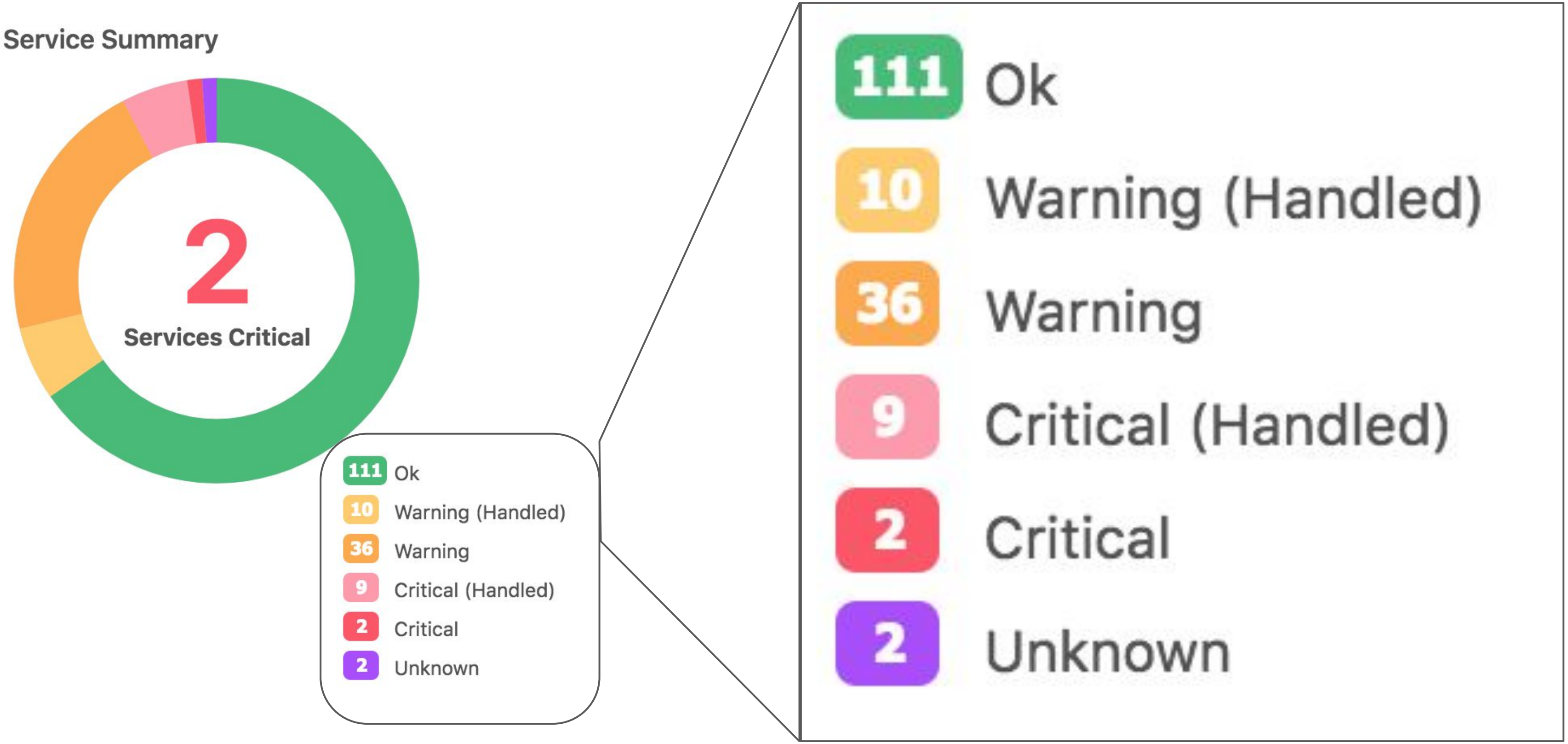
- *Liberating developers gave us creativity and ownership*
- *However, soon the time came to install guard rails*
- *A wrong turn should be hard to make*

Tracking Costs

What if we spun a web?



Governing Security



111	Ok
10	Warning (Handled)
36	Warning
9	Critical (Handled)
2	Critical
2	Unknown

111 Ok
10 Warning (Handled)
36 Warning
9 Critical (Handled)
2 Critical
2 Unknown

Can’t we all just get along?

- *Kubernetes - A multi tenant architecture*
- *Quotas should be clear and produce little to no overhead*
- *Teams should get a clear notification well before hitting their limits*

What’s next?

Better visibility

Tighter coupling

Back to where we started...

Should we monitor everything?

Can alerts suck less?

Who carries the pager?

Questions?

WORLD
CHMPS

Soluto

ICINGA

Thank You!

@yaronidan

@SolutoEng

Sources

Monitoring blog post at Soluto's engineering blog –

https://blog.solutotlv.com/distributed-monitoring-for-devops-teams-using-icinga-and-puppet/

https://github.com/Soluto/nagios-plugins

https://github.com/Icinga/puppet-icinga2

Tips and Tricks

Don’t let alert fatigue get you! Adjust alerts to only fire when disaster strikes

Learn from outages - make sure alerts were firing, and if they don’t - make‘em!

Choose a solution that allows versioning, preferable using monitoring-as-code

Use templating for apps that share the same monitoring patterns

Share the joy of holding a pager with your fellow developers

Focus your monitoring efforts on metrics that can harm your business