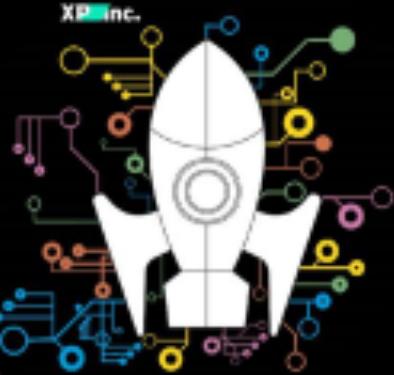


Hackathon TECH

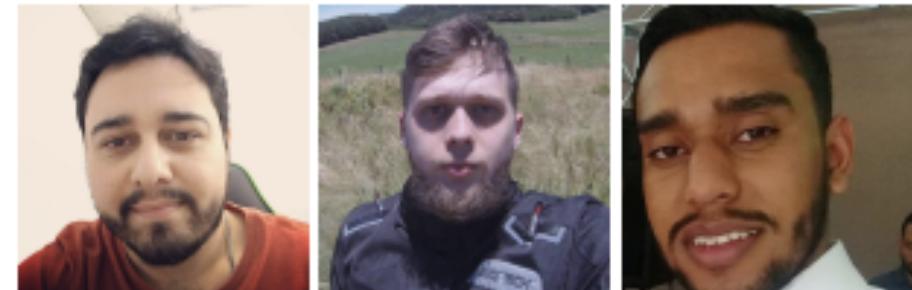
Freedom

XP inc.

Time is the greatest innovator.
Francis Bacon, 1625



Guilherme Oliveira – **Tech Leader**



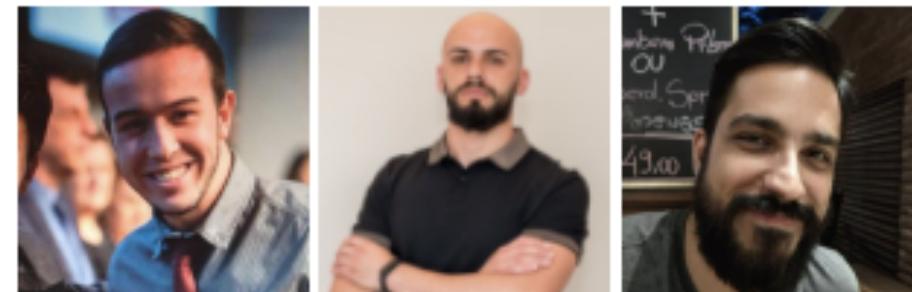
Willian Rempp – **Desenvolvedor**

Elias Neves – **Infraestrutura**

Victor Rizzo – **Infraestrutura**

Douglas Hermann - **Desenvolvedor**

Luiz Ihara - **QA**



De tempos em tempos, time de NOC sofre com massiva de alarmes no Zabbix.

Quando inicia a massiva de alarmes, o time inteiro tem que parar de realizar suas tarefas para ajudar nas analises, tratativas e contatos com as áreas.

1

Demora no tempo da tratativa de cada chamado

2

Alocação de recursos para ajudar na tratativa dos chamados

3

Quanto maior o tempo perdido, maior o prejuízo financeiro

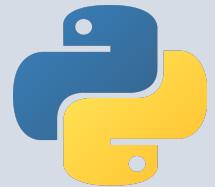
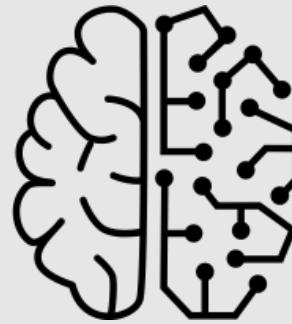
4

Impacto na imagem da empresa



Analisa a massiva de alarmes via **Machine Learning**,
Correlaciona os grupos,
Abre chamado no ServiceNow e
Entra em contato com as áreas responsáveis.





Python



Flask



docker

ZABBIX

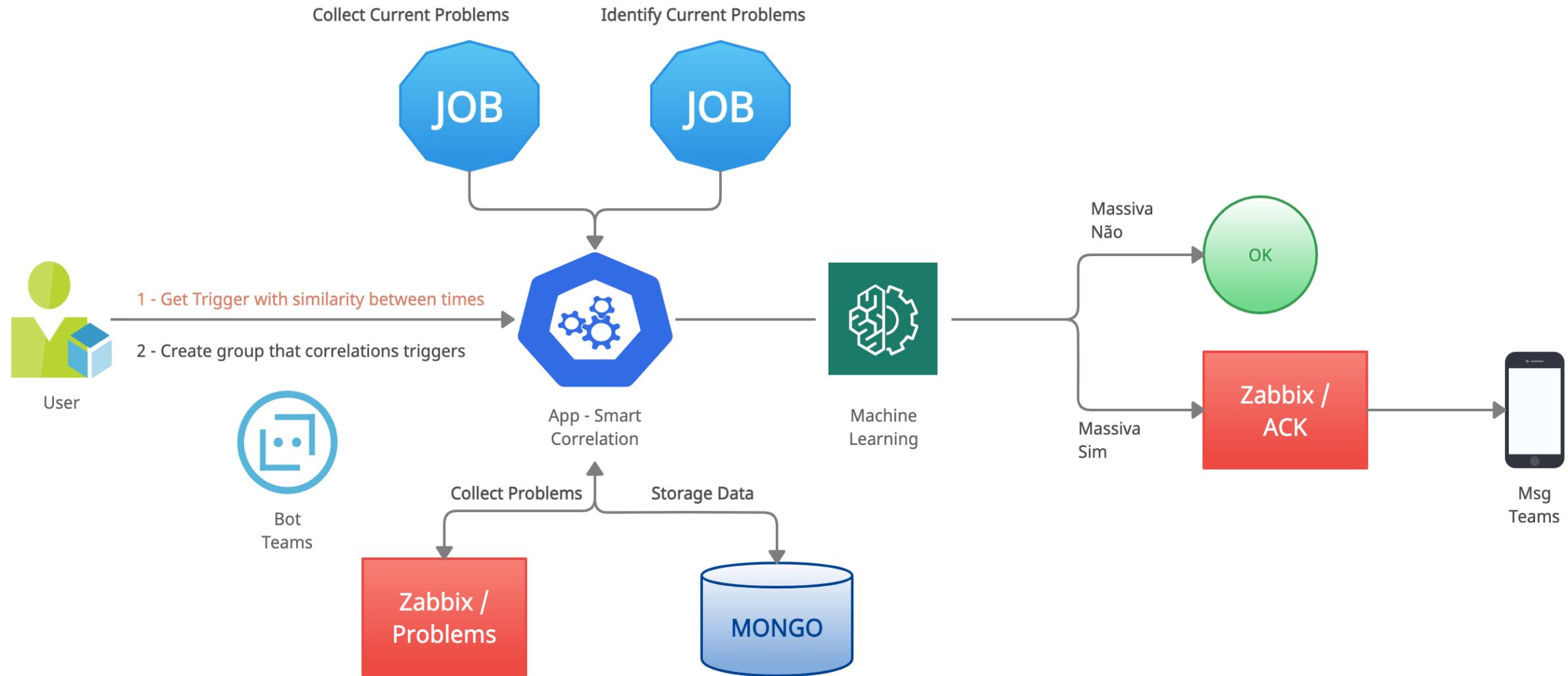


Microsoft Teams

servicenow.[®]

Como funciona?

Fluxograma



No Cenário Antigo, NOC iria analisar alarme por alarme para entrar em contato

Time	Info	Host	Problem	Severity	Duration	Ack	Actions	Tags
21:55:32	azhhackaton06	Item 11	azhhackaton06	Item 11	33s	Yes	1	1
21:55:32	azhhackaton06	Item 10	azhhackaton06	Item 10	33s	Yes	1	1
21:55:32	azhhackaton06	Item 9	azhhackaton06	Item 9	33s	Yes	1	1
21:55:32	azhhackaton06	Item 8	azhhackaton06	Item 8	33s	Yes	1	1
21:55:32	azhhackaton06	Item 7	azhhackaton06	Item 7	33s	Yes	1	1
21:55:32	azhhackaton06	Item 6	azhhackaton06	Item 6	33s	Yes	1	1
21:55:32	azhhackaton06	Item 5	azhhackaton06	Item 5	33s	Yes	1	1
21:55:32	azhhackaton06	Item 4	azhhackaton06	Item 4	33s	Yes	1	1
21:55:32	azhhackaton06	Item 3	azhhackaton06	Item 3	33s	Yes	1	1
21:55:32	azhhackaton06	Item 2	azhhackaton06	Item 2	33s	Yes	1	1
2m 3s No								
2m 3s No								

Antes

10 chamados P1 = 30 minutos

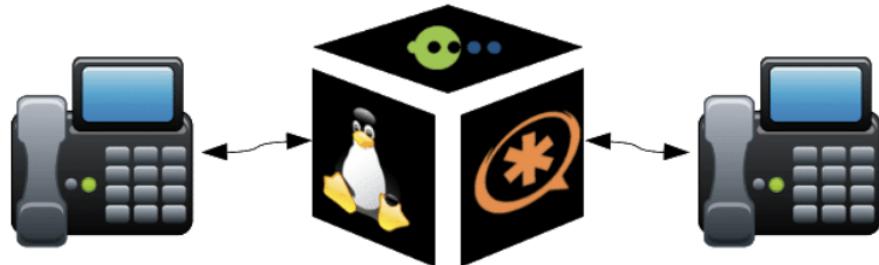
Depois

10 chamados P1 = 3 minutos

Nossa proposta é fazer com que o sistema identifique os relacionados, crie um chamado e entre em contato com os responsáveis.

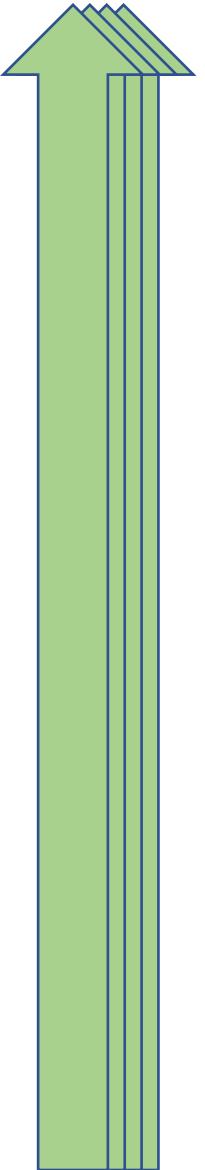
Acionamento via URA:

Ligaçāo automática para trigger que contenha incidente principal conforme correlaçāo feita pela aplicāção Smart Correlation.



Acionamento via BOT:

BOT do teams entrará em contato com o time, podendo receber ações.

- 
1. Agilidade no acionamento
 2. Acionamento automático
 3. Ganho de tempo para resolução do alarme
 4. Menor prejuízo para empresa
 5. Menor a alocação de recursos para ajudar na tratativa
 6. Subir o SLA de acionamento para maior que 95%



OBRIGADO

XP Inc.

