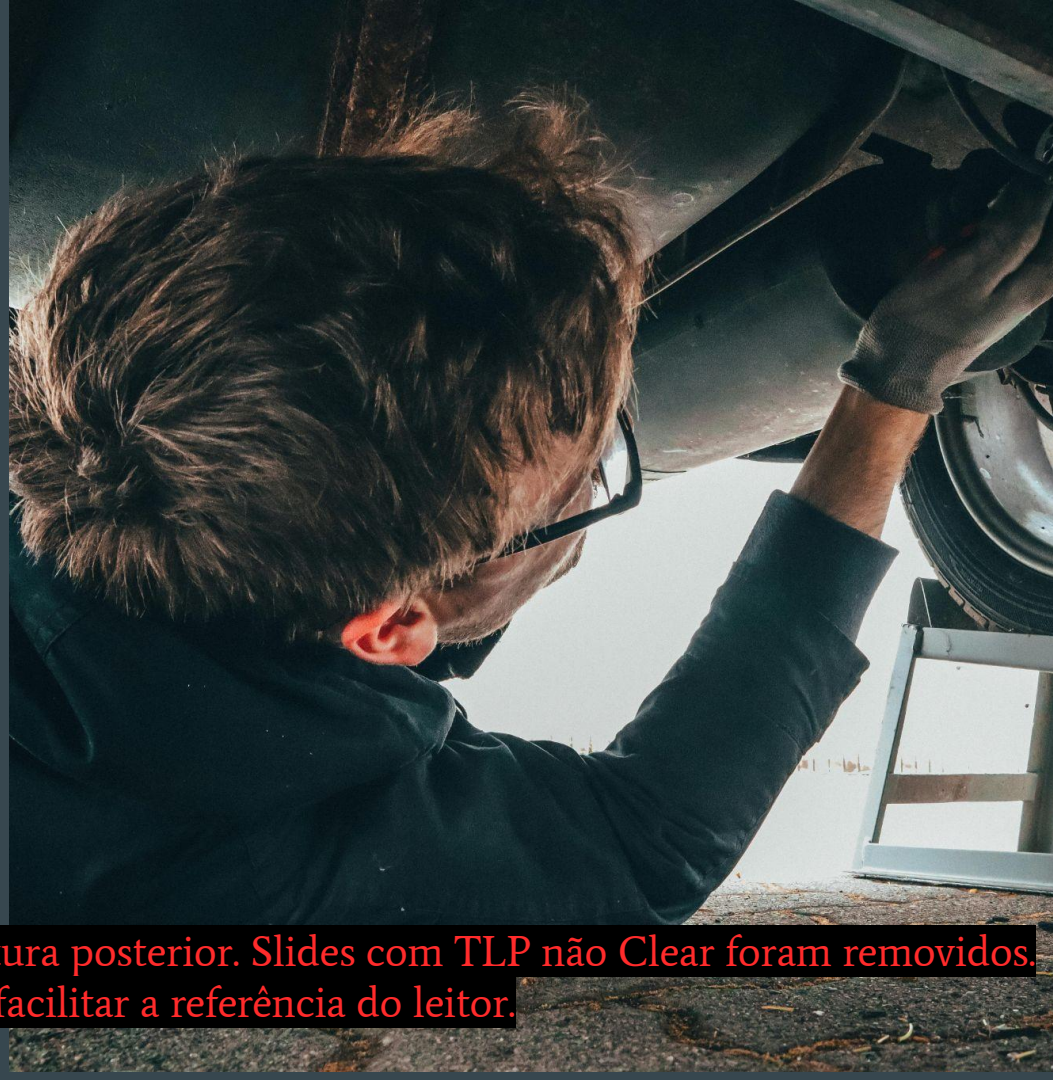
Trocando o motor do SOC

Insights sobre a mudança de plataformas de suporte ao SOC.



Esta versão foi modificada para facilitar a leitura posterior. Slides com TLP não Clear foram removidos. Adicionei alguns comentários do autor para facilitar a referência do leitor.

Eu

- Pai do Joaquim e do João.
- Especialista em Resposta à Incidentes.
- Gerente de plataformas para o SOC.
- Membro do First.org e colaborador ativo do SIG de Metrics.

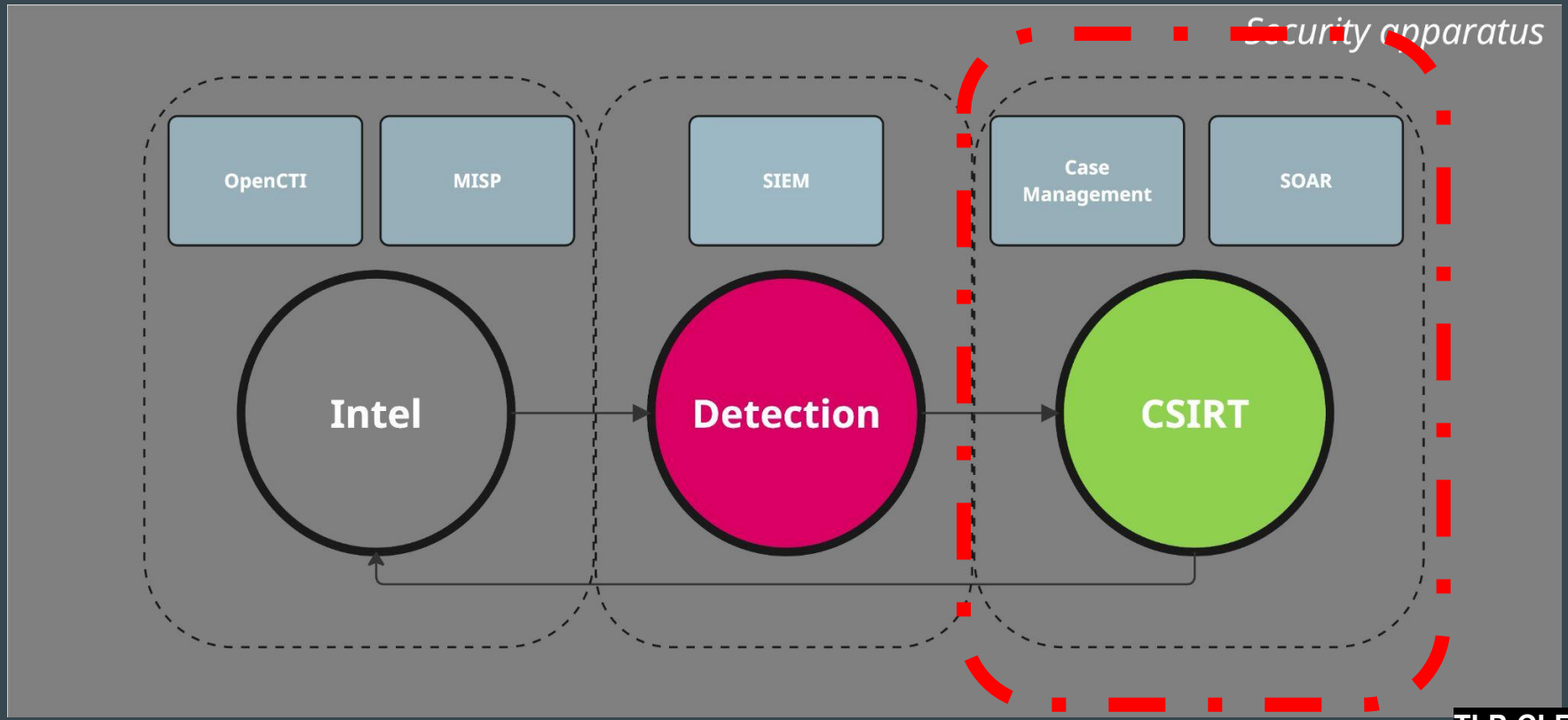
https://www.linkedin.com/in/romrocha/

TLP:CLEAR

Objetivos

- Com esta apresentação pretendo trazer, a observação do meu ponto de vista sobre a mudança de plataformas fundamentais para o ecossistema de um SOC. Essas observações são estritamente pessoais e tem correlação entre experiências passadas, pesquisas e idéias para o futuro.
- Quais os motivos de criar uma nova solução?
- O processo de descoberta e o racional para uma nova solução utilizando-se uma RFC.
- Alguns resultados

SOC Platform



TLP:CLEAR

Escalando o SOC

e criando PROBLEMAS...

TLP:CLEAR

Como escalar sem aumentar complexidade?

Como empoderar os analistas de resposta à incidentes a tornar seu trabalho mais eficiente?

Como escalar e acelerar minha resposta à incidentes de forma sustentável?

TLP:CLEAR

Buscando respostas...

Construindo uma RFC...

TLP:CLEAR

Engenharia de Segurança

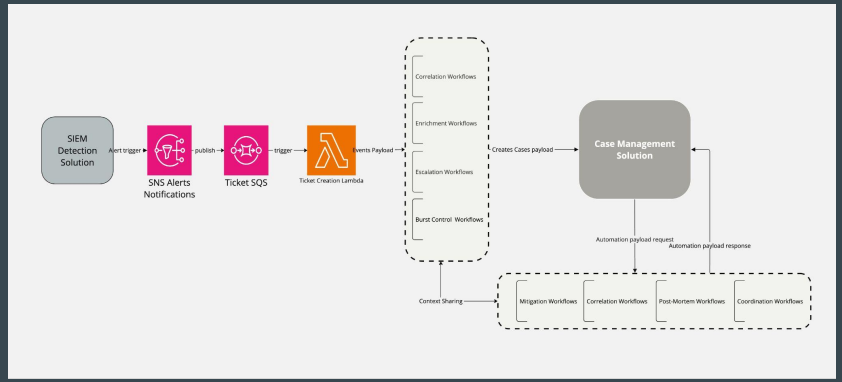
Um processo de construção de uma RFC foi iniciado no qual pretendemos explorar o que as possíveis soluções para os problemas.

O que idealmente deve conter um documento de RFC?

- Os problemas, fatos e a necessidade de solução.
- O que ela não pretende resolver.
- Perguntas em aberto.
- Alternativas e seus trade-offs.
- Compartilhamento com os pares e principais stakeholders para comentários e refinamento das necessidades.
- E finalmente a abordagem escolhida e seus detalhes.

TLP:CLEAR

Engenharia de Segurança



Problemas: Escalabilidade, Confiança e Eficiência.

Necessidades:

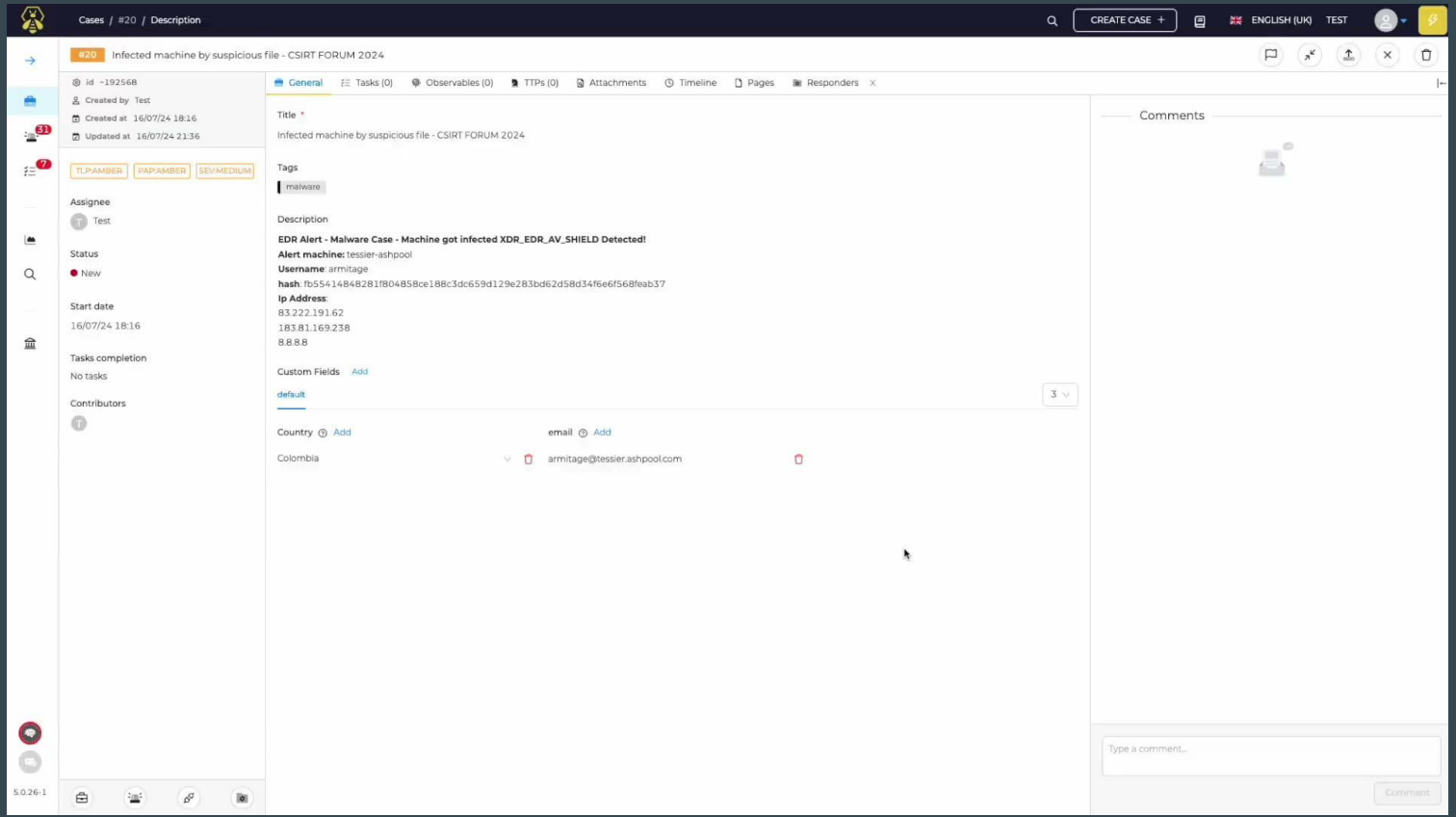
- Ter o contexto de diversas fontes unificadas nas mãos do analista.
- Ser flexível o suficiente para acomodar novas demandas do negócio.
- Ser uma solução que permita integração rápida e constante com novas ferramentas.
- Com características "universais" de resposta à incidentes.
- Tornar mais rápido o processo de desenvolvimento de automação, para novos entrantes .

Alternativas : Testar diferente combinações e levantar sobre seus trade-offs. (SOAR e Case Management)

TLP:CLEAR

POC - Como empoderar analistas de resposta à incidentes a serem mais eficientes?

TLP:CLEAR



O vídeo será disponibilizado no Linkedin.

TLP:CLEAR

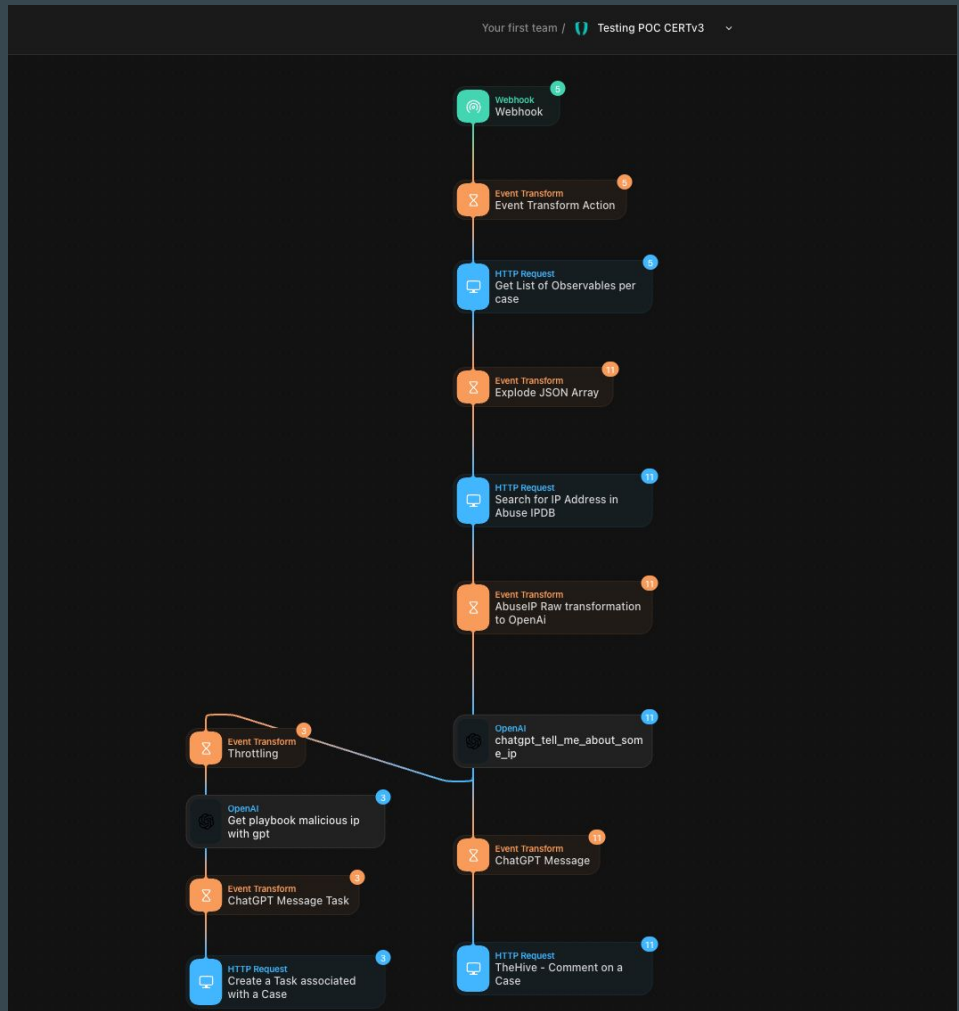
LOW CODE
Rápida solução.

Este é um workflow de exemplo do motor que realizou a automação no vídeo anterior. O The Hive foi configurado para enviar um evento (POST) ao webhook preparado para receber os eventos na ferramenta Tines.io (Community Edition).

Após a etapa anterior, todo o fluxo se dá através do workflow no Tines.io, (**existem diversas outras ferramentas, verifique o slide de referências)

Você pode baixar o JSON para testes e importar na sua instância de teste do Tines:

https://github.com/romrocha/csirt-workflows-poc/blob/master/tines_testing-poc-forum_csirt2024.json



TLP:CLEAR

Exemplos dos eventos


```
"chatgpt_tell_me_about_some_ip": {
    "body": {
        "id": "chatcmpl-9lnNprB67ywb6v66ZRGOXQ4JVCCen",
        "object": "chat.completion",
        "created": 1721178273,
        "model": "gpt-3.5-turbo-0125",
        "choices": [
            {
                "index": 0,
                "message": {
                    "role": "assistant",
                    "content": "Com base nas informações fornecidas, o endereço IP 183.81.169.238 parece ser de alto risco, com um
                    Abuse_Confidence_Score de 100. Isso sugere que há uma alta probabilidade de que este IP esteja envolvido em atividades de abuso.
                    Portanto, é recomendável ter cautela ao interagir com esse endereço IP e considerar sua segurança ao fazê-lo."
                },
                "logprobs": null,
                "finish_reason": "stop"
            }
        ],
        "usage": { ... },
        "system_fingerprint": null
```

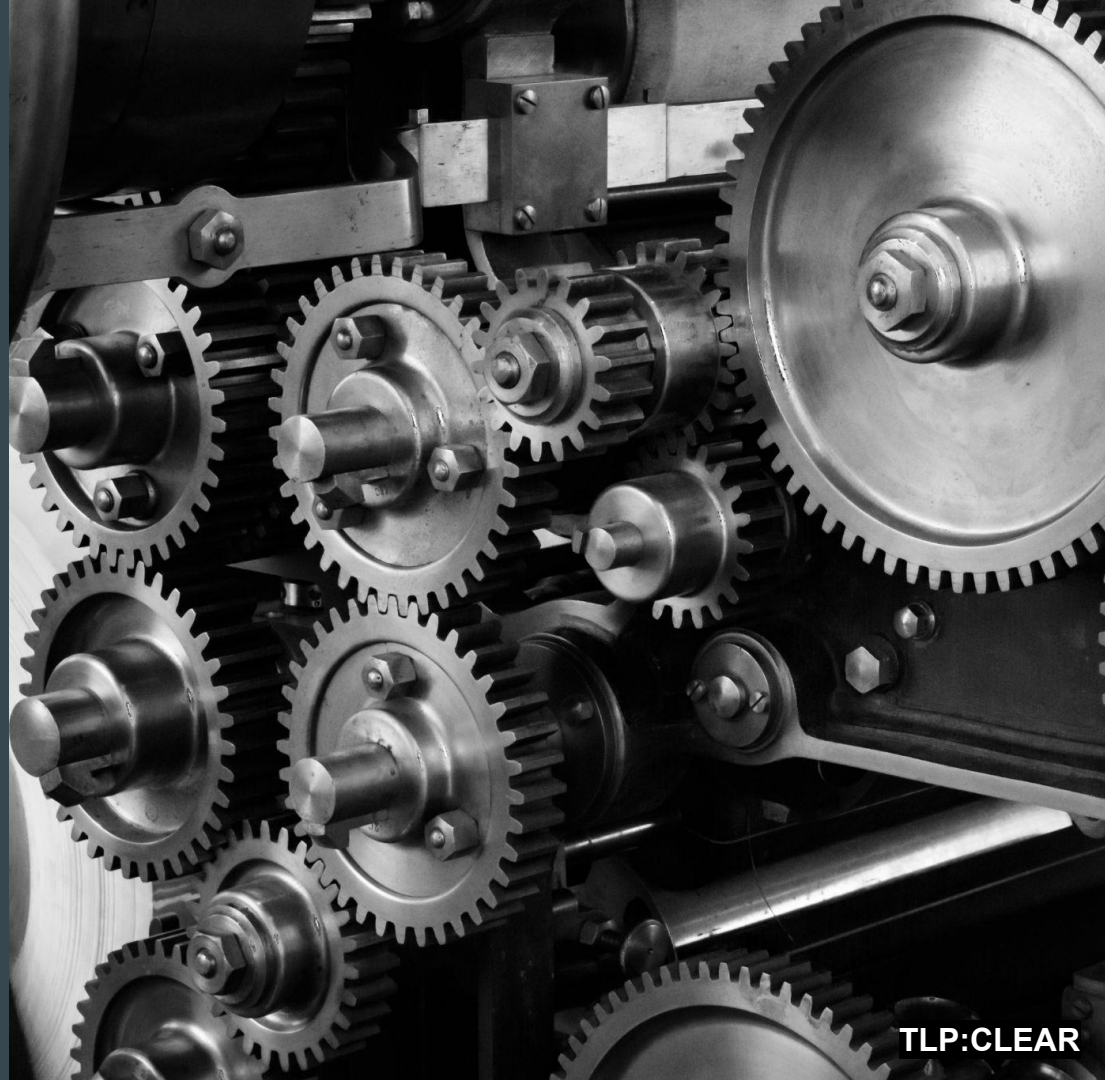
```
"event_transform_action": { ... },
"get_list_of_observables_per_case": {
  "body": [
    {
      "_id": "~82874584",
      "_type": "Observable",
      "_createdBy": "testing@test.com.br",
      "_createdAt": 1721178132813,
      "dataType": "ip",
      "data": "183.81.169.238",
      "startDate": 1721178132813,
      "tlp": 2,
      "pap": 2,
      "tags": [ ... ],
      "ioc": false,
      "sighted": false,
      "reports": { ... },
      "message": "Comecei uma investigação e me deparei com estes endereços, favor verificar.↵Rômulo Rocha",
      "extraData": { ... },
      "ignoreSimilarity": false
    },
    {
      "_id": "~41484352",
      "_type": "Observable",
      "_createdBy": "testing@test.com.br",
      "_createdAt": 1721178132765,
      "dataType": "ip",
      "data": "83.222.191.62",
      "startDate": 1721178132765,
      "tlp": 2,
      "pap": 2,
      "tags": [ ... ],
      "ioc": false,
      "sighted": false,
      "reports": { ... },
      "message": "Comecei uma investigação e me deparei com estes endereços, favor verificar.↵Rômulo Rocha",
      "extraData": { ... },
      "ignoreSimilarity": false
    },
```

```
"isPublic": true,
"ipVersion": 4,
"isWhitelisted": false,
"abuseConfidenceScore": 100,
"countryCode": "HK",
"usageType": "Data Center/Web Hosting/Transit",
"isp": "Amarutu Technology Ltd.",
"domain": "koddos.com",
"hostnames": [ ... ],
"isTor": false,
"countryName": "Hong Kong",
"totalReports": 185022,
"numDistinctUsers": 997,
"lastReportedAt": "2024-07-17T01:03:57+00:00",
"reports": [
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
    { ... },
```


TLP:CLEAR

Um novo motor

Soluções.



Obrigado

Obrigado ao meu time e a todos que colaboraram com essa palestra.
(Daniel Oliveira, Giancarlo, Leandro Rocha e João Ceron).

TLP:CLEAR

Referências

- https://blog.pragmaticengineer.com/rfcs-and-design-docs/
- https://blog.pragmaticengineer.com/scaling-engineering-teams-via-writing-things-down-rfcs/
- https://philcalcado.com/2018/11/19/a_structured_rfc_process.html
- https://www.paloaltonetworks.com/blog/2024/04/cybersecurity-platformization/
- https://www.redhat.com/pt-br/topics/automation/what-is-event-driven-automation
- https://www.industrialempathy.com/posts/design-docs-at-google/
- https://shuffler.io ("new" SOAR category)
- https://tines.io ("new" SOAR category)
- https://torq.io ("new" SOAR category)
- https://mindflow.io ("new" SOAR category)
- https://platform.openai.com/docs/api-reference/chat/create (open ai to "talk" with the model, 5$ cost)
- https://www.abuseipdb.com/api.html (you can use it for free)
- https://strangebee.com/ (TheHive case management platform)
- https://github.com/romrocha/csirt-workflows-poc/blob/master/tines_testing-poc-forum_csirt2024.json (my repo with json example to use in Tines.io)

TLP:CLEAR