Introdución

As novas tecnoloxías e comunicacións están cada día máis presentes en todos os ámbitos da sociedade. Do mesmo xeito, tamén os riscos asociados ao seu uso, por iso, cada día cobra máis importancia a seguridade informática.

Entidades privadas, públicas e corpos e forzas dos estados comezan a implementar diversas estratexias para protexer a súa infraestrutura, isto é, abarca desde os usos persoais até o esquema de seguridade estatal.

A seguridade informática é unha area de coñecemento moi ampla e soe dividirse de diversos xeitos, como poden ser: programación segura, auditoría, consultaría, ciberintelixencia, forense, resposta a incidentes, *red teams*, *blue teams*, etc.

A ciberintelixencia é unha especialización que cada día cobra máis protagonismo, non só pola necesidade de xente que se adique a ela, senón pola súa importancia noutras especializacións destacando o OSINT (Open Source Intelligence, Intelixencia de fontes de datos de libre acceso) e a recolección de IOCs (Indicators of Commitment), utilizados por motores de sistemas *antimalware*, para buscar ameazas coñecidas en procesos de investigacións forense ou en actividades diarias como o Threat Hunting e o Retro-Hunting.

O Threat Hunting é a actividade de buscar posíbeis vías de entrada a unha infraestrutura por parte de atacantes que están intentando utilizar ferramentas, vulnerabilidades ou *malware* coñecido. Isto é, atopar onde pode que fallen as medidas de seguridade despregadas.

O Retro-Hunting é a actividade que, unha vez se actualiza a base de coñecemento con IOCs, buscar na infraestrutura se se chegou a estar comprometido nalgún momento.

O ámbito deste TFG (Traballo de Fin de Grao) é realizar un *framework* que facilite a labor de ciberintelixencia de recolección de IOCs para poder ser utilizados por equipos CERT/CSIRT (Computer Emergency Response Team/Computer Security Incident Response Team) en tarefas de análise forense, Hunting e Retro-Hunting.

Obxectivos

Este TFG ten como obxectivo principal a creación dun *framework* para ciberintelixencia que permita:

- Dispor dunha fonte de coñecemento alimentada de diversas fontes como:
  - MISP (Malware Information Sharing Plataform): http://www.misp-project.org/
  - TotalHash: https://totalhash.cymru.com
  - VirusSign: http://www.virusign.com/
  - VirusShare: https://virusshare.com/
- Unha API que permita:
  - Realizar consultas á base de coñecemento mediante diferentes criterios: nome do binario, *hash*, IP, dominio, etc.
  - Engadir IOCs propios.
  - Solicitar o resultado en formatos diferentes como: JSON, Yara Rules, XML, Splunk Query, etc.

Descrición técnica

Realizarase un *framework* en python onde se definirán puntos de extensión que permitan:

1. Engadir diversos *feeds* dos citados no punto anterior para alimentar a base de datos de IOCs.
2. Consumir a base de coñeemento de IOCs de diversas formas.

O núcleo deste *framework* será unha base de datos non relacional (MongoDB), onde se almacenarán os IOCs coñecidos e onde se irán engadindo a diario os novos IOCs.

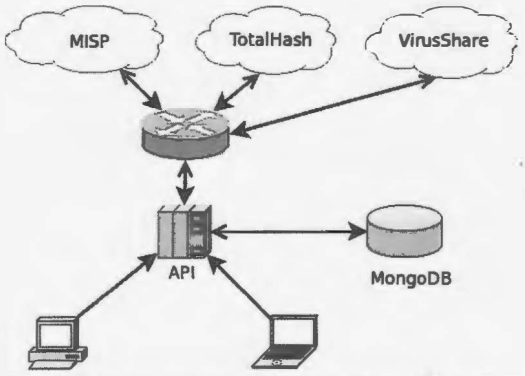

Ilustración 1: diagrama da estrutura do proxecto

Metodoloxía de desenvolvemento

Para o proceso de desenvolvemento deste TFG empregarase a metodoloxía áxil Scrum, baseada nun modelo de proceso iterativo e incremental.

As iteracións en Scrum coñécense como *sprints* e teñen a particularidade de engadir algunha condición adicional, como que o tempo máximo para a súa realización é dun mes ou, quizais máis importante, que deben incluír as seguintes reunións:

- Sprint Planning: realizase ao comezo de cada *sprint* e nela determínanse as funcionalidades a desenvolver no *sprint*.
- Diaria (Daily Meeting): reunión diaria na que o equipo de desenvolvemento pon en común o traballo realizado e o traballo que se vai realizar durante a xornada laboral. Neste caso establécese como semanal, debido ao tamaño reducido do equipo de desenvolvemento. Ademais, estará orientada a pór común o traballo que se realizou na última semana, o que se realizará na próxima semana e se houbo algún impedimento para levar a cabo o obxectivo marcado.
- Sprint Review: revísase que foi e que non foi completado e presentarase o traballo completado ao cliente e usuarios. É un punto para obter retroalimentación sobre o produto.
- Sprint Retrospective: os membros do equipo de desenvolvemento valorarán o *sprint* co fin de realizar unha mellora continua no proceso.

Por outra banda, nun Equipo de Scrum existen tres roles:

- Product Owner: o propio cliente ou un representante do mesmo que entenda ben o modelo de negocio.
- Scrum Master (Facilitador): é quen se encarga de eliminar os obstáculos que poidan impedir que se leve a cabo o *sprint* e asegura que o proceso de Scrum se realice como é debido.
- Development Team (Equipo de Desenvolvemento): responsable de desenvolver e entregar o produto.

Neste TFG o Equipo Scrum só constará dos titores, que exercerán de Product Owner e Scrum Master, e do alumno, que exercerá en solitario de Development Team en lugar dos 3 a 9 que recomenda Scrum.