

#Compartiendo Conocimiento

#Inteligencia Colectiva



IntelCon
by Ginseg

Hackathon

Congreso Online de **Ciberinteligencia**

28 de septiembre al 3
de octubre **2020**

Normas y bases del **Hackathon**

Con esta Hackathon se pretende favorecer el crecimiento de la comunidad de Ciberinteligencia Ginseg, por lo que se propone desarrollar una solución enfocada en éste ámbito de la ciberseguridad, que resuelva alguna carencia existente en las herramientas o soluciones actuales, o mejore las prestaciones de alguna de ellas.

1. El tamaño mínimo de participantes por equipo es de **3**, y no podrán superar los **5 miembros**. No podrán formar parte de ningún equipo los miembros colaboradores de la comunidad.
2. Se recomienda formar equipos multidisciplinares, para elaborar una solución lo más completa posible.
3. Todos los miembros del equipo deben estar registrados en la competencia.
4. Los equipos pueden obtener asesoramiento externo, pero la propiedad intelectual de la solución debe pertenecer al equipo.
5. La solución propuesta debe incluir como mínimo uno de los siguientes ciclos de CiberInteligencia:
 - **Dirección y planificación**
 - **Obtención**
 - **Análisis y elaboración**
 - **Difusión**
6. Todo el trabajo debe realizarse únicamente durante el periodo que dure la Hackathon (**desde las 00:00 de España del día lunes 28 de septiembre hasta a las 18:30 de España del día sábado 3 de octubre**)
7. Los equipos pueden proponer una solución para participar, o elegir una de las propuestas por la organización.
8. Los equipos subirán el código al repositorio de Github dispuesto para este fin. (**Leer Disclaimer**)
9. Los equipos pueden utilizar las librerías o *frameworks* que consideren, siempre que se cumplan las normas para liberar el código, dispuestas en el *disclaimer*.
10. Los proyectos que incumplan alguna de las normas no serán tomados en cuenta.
11. La organización se guarda el derecho de descalificar a los equipos en caso de infracción de las normas, realización de prácticas abusivas.
12. La demostración se realizará frente al tribunal dispuesto por la organización, que serán los encargados de valorar el trabajo realizado.
13. La demostración no podrá superar los **15 minutos** por equipo.
14. La demostración puede constar de cualquier representación que favorezca la comprensión de la solución, como, vídeo, imágenes, presentación en vivo del funcionamiento, PowerPoint, etc.
15. Se evaluará cada propuesta basada en los criterios de evaluación descritos en la descripción de la Hackathon.

Premios Hackathon

Hackathon IntelCon tiene una serie de premios en función de la valoración final por parte del jurado. Los equipos ganadores dispondrán de los premios en forma de formación sobre diversas disciplinas (OSINT, SOCMINT, Deep Web, etc) y técnicas de análisis de inteligencia, además de una serie de horas de mentoring con los fundadores de la comunidad GINSEG. Los premios podéis verlos en el ranking inferior en relación al primer, segundo y tercer puesto.

1er Puesto

Beca parcial para el Master de Ciberinteligencia



5 horas de mentoring con fundadores GINSEG

2do Puesto

Descuentos del 50% en formación con I+L



2 horas de mentoring con fundadores GINSEG

3er Puesto

Descuentos en formación con Cyber Hunter Academy



1 hora de mentoring con fundadores GINSEG

Sistema de puntuación y valoración del **Hackathon**

Al culminar el plazo para la entrega de tu propuesta, tendrás **15 minutos** para presentarla ante un jurado de expertos compuesto por Wiktor Nykiel, Raúl Renales, Pablo San Emeterio, Juan Antonio Calles, además de un voto por parte de la comunidad pertenecientes a GINSEG.

Criterio 1: Ambición del problema

Escala y complejidad del problema a explorar.

Criterio 2: Innovación de la solución

Escala, diseño e innovación de la tecnología que se usa.

Criterio 3: Calidad del código

Esta categoría consiste en medidas subjetivas que definen una buena pieza de código como la mantenibilidad, legibilidad y formato del código, claridad, testing efectivo del software y eficiencia.

Criterio 4: Calidad de la implementación

Habilidad para el equipo para lograr una conclusión acerca de la viabilidad del proyecto.

Criterio 5: Impacto a la Ciberinteligencia

El impacto y aporte que la solución proporciona al campo de la Ciberinteligencia.

Criterio 6: Calidad de la Presentación

Habilidad del equipo para presentar los resultados obtenidos, tanto la funcionalidad esperada, como el comportamiento final obtenido en la solución.

#InteligenciaDeAmenazas #OSINT #SOCMINT #VirtualHUMINT
#DeepWeb #RespuestaIncidentes #TécnicasAnálisis #Herramientas #Ciberamenazas

La asistencia es totalmente gratuita para los asistentes y 100% en streaming online.

 CN-CERT
centro criptológico nacional incibe_
INSTITUTO NACIONAL DE
CIBERSEGURIDAD

Ideas a implementar en el Hackathon

En el caso de que no se disponga de una idea sólida sobre que proyecto realizar, os facilitamos una serie de ideas de proyectos a continuación:

1. Proactive CTI IOCs

Los indicadores de compromiso proactivos son aquellos que están basados en la detección temprana de riesgos que puedan significar una potencial amenaza a la seguridad de cualquier compañía. El reto principal es desarrollar una idea (herramienta) para la generación automática de Indicadores de Compromiso proactivos a partir de procedimientos de obtención de información de fuentes abiertas (OSINT) o redes sociales (SOCMINT) y usando técnicas como Scraping, Crawling, NLP o el uso de APIs abiertas.

En este reto se evaluará principalmente el valor que los IOCs generados pueden brindar a una compañía, también se evaluará las fuentes de donde la información es obtenida y su relevancia para aportar información sobre potenciales amenazas. Todos los miembros del equipo deben estar registrados en la competencia.

3. Report Framework:

La elaboración de informes corporativos es esencial para presentar, de una forma resumida, los resultados de los análisis y procedimientos llevados en una investigación de inteligencia, muchas veces la elaboración de estos informes puede ser tediosa y ocasionan una pérdida de tiempo que se puede aprovechar en otras investigaciones. El reto principal es desarrollar una idea (herramienta) que, a partir de una plantilla, facilite la generación rápida de estos informes con una presentación clara y concluyente de la investigación llevada a cabo.

En este reto se valorará la capacidad de la herramienta para generar un informe rápido, sencillo y de contenido de calidad que resuma claramente la investigación realizada.

2. APT Framework

Las amenazas que representan los grupos APT para cualquier compañía o infraestructura crítica pueden llegar a ser devastadores ya que combinan técnicas avanzadas y persistentes para atacar a sus víctimas. El reto principal es desarrollar una idea (herramienta) que sea capaz de sincronizarse y alimentarse con información obtenida de plataformas como la matriz de MITRE ATT&CK, entre otras, para así identificar una posible amenaza temprana de este tipo basado en las tácticas, técnicas y procedimientos (TTPs) que caracterizan a cada uno de estos grupos APT.

En este reto se valorará la capacidad de la herramienta para detectar una posible amenaza de tipo APT a partir de los vectores de ataque que están afectando en el momento a una compañía.

Ginseg – IntelCon **Disclaimer**



¿Quiénes somos?

GINSEG es una comunidad de Ciberinteligencia, que pretende ser un nexo de unión entre las diferentes disciplinas de inteligencia y la ciberseguridad con el fin de fomentar la formación de calidad, el conocimiento compartido y colaborativo. Por ello se ha creado la primera edición del ciclo de conferencias IntelCon, para favorecer esta difusión de conocimiento y como punto de encuentro entre todas las personas interesadas. Y dentro de este ciclo, se propone entre otras cosas un Hackathon, donde todos los participantes pueden demostrar sus habilidades y cuya finalidad no es otra que apoyar a la creación de contenido de la comunidad.

Condiciones de uso

GINSEG en IntelCon 2020 ofrece acceso a su repositorio Github <https://github.com/intelcon2020> para todos aquellos equipos que deseen participar en el Hackathon, en las condiciones de uso que se describen a continuación:

Equipos participantes

Los equipos que se presenten como participantes al Hackathon deben aceptar las condiciones de uso descritas en el presente documento, especialmente los apartados de “Derechos de propiedad intelectual” y “Exclusión de garantías y responsabilidades”.

Usuarios

El acceso a los recursos del repositorio atribuye a quien lo realiza la condición de Usuario, y asume aceptación plena de las condiciones de uso descritas en el presente documento, especialmente los apartados de “Contenido y uso adecuado” y “Exclusión de garantías y responsabilidades”

Derechos de propiedad intelectual

Todos los proyectos alojados en el repositorio de Github, así como nombres comerciales, marcas o distintivos generados durante el Hackathon estarán protegidos mediante propiedad intelectual y sus derechos pertenecerán única y exclusivamente a sus creadores, es decir, a todos los equipos o desarrolladores participantes del Hackathon.

Sin embargo, se ruega que el trabajo realizado durante la competición se libere bajo una licencia “Open Source” / libre, permitiendo que las herramientas desarrolladas favorezcan el crecimiento de la comunidad GINSEG.

Contenido y uso adecuado

Las herramientas alojadas en el repositorio dispuesto en para el Hackathon estarán disponibles para toda la comunidad, con el fin de facilitar su acceso y distribuir el conocimiento generado durante las jornadas IntelCon.

GINSEG aboga siempre por un uso adecuado de los recursos expuestos.

Exclusión de garantías y responsabilidades.

GINSEG no se responsabiliza de los contenidos generados durante el Hackathon en el repositorio. Si en algún momento se detectase o fuese reportado algún código malicioso, será revisado, notificado y eliminado del repositorio. De la misma manera, GINSEG no se responsabiliza del uso que se le puedan dar a las herramientas que se expongan en el repositorio, pero insiste en que están pensadas para el desarrollo de la comunidad de Ciberinteligencia.

Las presentes condiciones de uso se registrarán por lo dispuesto en la legislación española.