MAESTRÍA EN CIBERSEGURIDAD

INFORME DE INVESTIGACIÓN

TÍTULO: “Optimización del Proceso de Cacería de Ciber Amenazas Obscuras en la Red, a Través del Uso de Indicadores de Compromiso y Fuentes de Amenazas.”

Alumno: Msc. Marco Antonio Cevallos Moreno.

Tutor: Dr. Sebastián Tamayo.

Quito, mayo de 2021

ABSTRACT

En el ámbito de Ciber Seguridad, existen un sin número de criterios y políticas que definen en las empresas, los métodos para realizar cacería de amenazas cibernéticas. El objetivo de este trabajo es plantear un esquema que permita a una empresa optimizar la manera en la que puede realizar sus actividades de identificación de una amenaza cibernética, así como realizar un triage en menor tiempo.

In the Cyber Security field, there are a number of criteria and policies which define, the methods for cyber threat hunting. The objective of this work is to propose a scheme which allows a company to optimize the way they carry out its activities to identify a cyber-threat, as well as perform cyber threat triage in less time.

PALABRAS CLAVE

Inteligencia de amenazas, cacería de amenazas, indicadores de compromiso, firma,

ciber amenaza.

Threat intelligence, threat hunting, indicators of compromise, sign, ciber threat.