UNIVERSIDAD PERUANA DE LAS AMÉRICAS

ESCUELA PROFESIONAL DE INGENIERIA COMPUTACIÓN Y SISTEMAS

TRABAJO DE INVESTIGACIÓN

IMPLEMENTACIÓN DE UN CENTRO DE OPERACIONES DE CIBERSEGURIDAD (SOC) PARA MEJORAR LA DETECCIÓN DE ATAQUES CIBERNÉTICOS EN EMPRESAS DEL SECTOR TECNOLÓGICO, LIMA-2022.

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE COMPUTACIÓN Y SISTEMAS

AUTOR:

CISNEROS HENRIQUEZ PAULO CESAR

CÓDIGO ORCID: 0000-0003-3923-6152

ASESOR:

Dra. NEGRÓN MARTINEZ CONSUELO CARMEN

CÓDIGO ORCID: 0000-0001-6911-8101

LINEA DE INVESTIGACIÓN: INTELIGENCIA ARTIFICIAL Y GESTIÓN DE INFORMACIÓN

LIMA – PERÚ

2022

Dedicatoria

A mis padres, por guiarme hasta aquí, también a mi esposa e hija por su apoyo incondicional de todo los dias.

Resumen

El presente trabajo de investigación se implementó en un centro de operaciones de ciberseguridad (SOC) con herramientas Open Source, haciendo uso de las buenas prácticas de los estándares internacionales como ISO/IEC: 27035 “Gestión de Incidentes de Seguridad” y el Cybersecurity Framework del NIST.

La metodología que se utilizó fue inductiva ya que hoy en día los ciberataques están aumentando en gran medida y cada vez son más sofisticados lo que obliga a las áreas de TI a tomar conciencia de lo que está sucediendo e implementar medidas al respecto para contrarrestar este oleaje de ciber amenazas. Según Kaspersky Labs el Perú en febrero del 2020 registró 787,774 ataques cibernéticos los cuales ascendieron a 2.7 millones en marzo del mismo año, este aumento en definitiva fue mayor que el crecimiento global promedio registrado de 197% y para los primeros meses del 2021 ya se registraban 5.7 millones de ataques cibernéticos. Señala EY que el 60% de empresas Peruanas ya se preocupan por su capacidad de enfrentar ataques de ciberseguridad; sin embargo, la limitación económica podría verse involucrada en la decisión de implementación por falta de conocimiento de otras alternativas.

En conclusión, la implementación de un SOC con herramientas de libre costo aporta de manera significativa la detección y respuesta de los incidentes de ciberseguridad que día a día se producen y reproducen sobre cualquier sistema en línea. También cubre la necesidad del factor económico.

Palabras clave: *SOC, ciberseguridad, amenazas cibernéticas, detección y respuesta*

Abstract

The present research work was implemented in a cybersecurity operations center (SOC) with Open-Source tools, making use of the good practices of international standards such as ISO/IEC: 27035 "Security Incident Management" and the Cybersecurity Framework of the NIST.

The methodology that was produced was inductive since today cyber-attacks are greatly increasing and are becoming more sophisticated, which forces IT areas to become aware of what is happening and implement measures in this regard to counteract this wave. of cyber threats. According to Kaspersky Labs, Peru in February 2020 had 787,774 cyber-attacks, which amounted to 2.7 million in March of the same year, this increase was greater than the average global growth of 197% and for the first months of 2021 they were already registered. 5.7 million cyber-attacks. EY points out that 60% of Peruvian companies are already concerned about their ability to face cybersecurity attacks; however, the economic limitation could be involved in the implementation decision due to lack of knowledge of other alternatives.

In conclusion, the implementation of a SOC with free-cost tools significantly contributes to the detection and response of cybersecurity incidents that are produced and reproduced every day on any online system. It also covers the need for the economic factor.

Keywords: *SOC, cybersecurity, cyberthreats, detect and response*

Tabla de contenidos

Resumen ..... **iv**

Palabras clave ..... **iv**

Keywords ..... **v**

Introducción **1**

Antecedentes **2**

Desarrollo del tema **5**

Definición de términos básicos **8**

Justificación e importancia de la investigación **14**

Conclusiones **15**

Aportes de la investigación **16**

Recomendaciones **17**

Referencias **18**

Introducción

La presente investigación tuvo como objetivo implementar un centro de operaciones de ciberseguridad (SOC) para las empresas del sector tecnológico, el cual permitirá mejorar la detección de ataques cibernéticos correlacionando todos los eventos de seguridad (logs) que se almacenan en las herramientas de protección de seguridad implementadas (Firewall, WAF, AntiDDoS, Active Directory, etc.), Así mismo dicha implementación estará bajo la norma ISO/IEC: 27035: Gestión de Incidentes de Seguridad y alineada con el marco de buenas prácticas del Cybersecurity Framework NIST.

Con la implementación de este centro la organización tendrá visibilidad de todos los sucesos del tráfico de red y de cada uno de los equipos instalados que cumplen una función importante, bien puede ser servidores, equipos de red, servidores de directorio activo, servidor de antivirus, antimalware y cualquier otro equipo de red que se desee monitorear.

La solución propuesta está pensaba para llegar a empresas que no cuenten con recursos económicos suficientes para su implementación por ello se utiliza 100% software libre (Open-Source) el cual es fácil de implementar y muy provechoso al utilizar en las siguientes páginas se detallará toda la información de como un centro de operaciones de ciberseguridad (SOC) mejorará en gran medida la detección de ataques cibernéticos con el fin de aplicar una respuesta rápida a la contención y evitar que se materialice.

Antecedentes

Internacionales

Rodriguez (2020), indica en su investigación titulada “Implementación de las operaciones de un SOC en una institución financiera partiendo desde cero utilizando soluciones SIEM” de la base de datos de la Universidad Oberta de Catalunya, Catalunya, España. Comentó la necesidad de implementar un centro de operaciones de seguridad (SOC) con el objetivo de realizar un monitoreo de las múltiples amenazas cibernéticas actuales, tal implementación requiere del consumo de logs de los sistemas que almacenan cada proceso y suceso, este servirá como input para modelar casos de uso ante un comportamiento extraño en los sistemas y pueda ser alertado. También menciona que las empresas dedicadas al rubro financiero requieren de un centro de este tipo para cumplir con exigencias normativas dictadas por el gobierno, finalmente hace énfasis que la herramienta que utilizó para la gestión de eventos tiene un alto costo económico por lo tanto su implementación dependía netamente del presupuesto asignado.

Marquez et al. (2020), indica en su investigación titulada “Diseño de un security operations center (SOC), mediante la implementación de roles definidos por el instituto SANS proporcionando las funciones de recopilar y filtrar datos, detectar y clasificar amenazas, analizar e investigar amenazas y la implementación de medidas preventivas para la red de la unidad educativa salesiana maría auxiliadora - UESMA, ciudad de esmeraldas” de la base de datos de la Universidad Politécnica Salesiana Sede Quito, Quito, Ecuador. Discute que la implementación de este tipo de centros de operación de seguridad son necesarios para mejorar

el nivel de visibilidad y con ello el análisis con la investigación de los ciberataques que hoy en día son muy comunes y peligrosos, los autores consideraron aplicar esta solución basándose en los roles que otorga la SANS haciendo uso de la metodología “Prueba Piloto” consiguiendo finalmente la dimensión de la infraestructura que requiere dicha implementación, finalmente concluyen que este tipo de centros de operación aumenta en gran medida el grado de control, visibilidad y prepara a los equipos de seguridad informática para una adecuada respuesta ante un incidente crítico relacionado.

Nacionales

Vilcarromero et al. (2019), indica en su investigación titulada “Propuesta de implementación de un modelo de gestión de ciberseguridad para el centro de operaciones de seguridad (SOC) de una empresa de telecomunicaciones” de la base de datos de la Universidad Peruana de Ciencias Aplicadas (UPC), Lima, Perú. Comenta la importancia de la operación de los sistemas de seguridad de las organizaciones debido a que las abundantes amenazas de ciberataques cada vez aumentan, son complejas y tienen mayor eficacia, por lo tanto, es muy relevante determinar el nivel de madurez de estos centros de operación para evitar riesgos con impacto crítico. También menciona que hoy en día la información es un activo de suma importancia el cual su aseguramiento es fundamental en toda organización para lograr confianza con el cliente y asegurar la confidencialidad de esta en conjunto con la disponibilidad e integridad, finalmente concluyen que las implementaciones de estos centros de operación están respaldados siempre y cuando se implementen con marcos de trabajo internacionales como CSF del NIST los cuales contienen las buenas prácticas que asegurarán una correcta gestión.

Mendoza et al. (2019), indica en su investigación titulada “Evaluación de la capacidad de detección y respuesta a riesgos de ciberseguridad, caso de la empresa SISC” de la base de datos de la Universidad del Pacifico, Lima, Perú. Redacta la preocupación de las organizaciones en cuanto a las concurrentes amenazas de ciberataques que ponen en un continuo riesgo los sistemas informáticos e información que estos almacenan por lo tanto se hace necesario realizar la evaluación de la operación de detección y respuesta de un centro de operaciones de seguridad (SOC) para conocer el nivel de madurez de este. Para la evaluación se utilizaron estándares internacionales (NIST, ISO/IEC 33020-2015 y COBIT 5) los cuales aportan buenas prácticas firmes que garantizaron cubrir todo el alcance de ciberseguridad, tras la evaluación concluyeron que todos los procesos de gestión de un centro de operaciones de seguridad deben tener mantenimientos por lo menos 2 veces por año lo cual refuerza el nivel de madurez de este.

Desarrollo del tema

Descripción de la realidad problemática

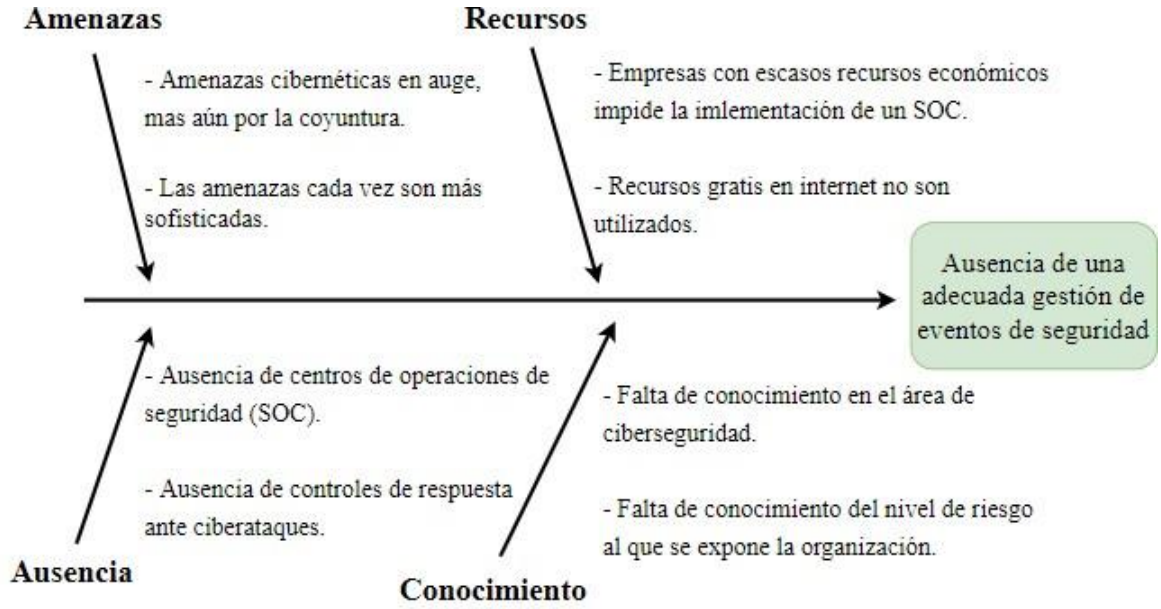
En estas épocas en donde ya nos encontramos viviendo la era de la cuarta revolución industrial, la tecnología avanza de manera impresionante, acorde a la misma también crecen en auge las amenazas cibernéticas que cada vez son más sofisticadas y dirigidas a objetivos en específico con un fin en la mayoría de los casos, monetarios. Ante esta creciente ola de amenazas las organizaciones optan por adquirir herramientas de protección con medidas que los ayuden a contrarrestar estas amenazas; sin embargo, muchas de ellas generan un acto de conformismo creyendo que es suficiente para la retención. Esto definitivamente no es suficiente ya que, si no existe una adecuada gestión de eventos, es decir; un centro de operaciones de seguridad (SOC) que constantemente monitoree y analice los sucesos es muy probable que le empresa sufra un ataque cibernético o quizás ya lo haya sufrido; pero este no ha sido detonado por el atacante ya que el objetivo es otro, sea cual sea el caso, el impacto en el negocio es crítico con posibilidades de quebrar y cerrar las operaciones.

Uno de los mayores problemas de las organizaciones es que no cuentan con personas especialistas en el área de ciberseguridad para poder realizar este tipo de evaluación y consigo la implementación de un centro de operaciones de seguridad adecuado para cubrir esta brecha importante, sumado a ello desconocen el nivel de riesgo al que se encuentran expuestos.

No estar capacitado en el área implica no tomar conciencia de las acciones de la administración de seguridad TI de la organización, sumado a ello las empresas que recién inician carecen de presupuesto económico destinado a este tipo de implementaciones, el mayor número de veces la inversión es puesta en el día a día (la operación) dejando de lado la seguridad, no obstante

existen recursos de uso gratuito en internet que pueden cubrir esta importante ausencia de gestión; sin embargo una vez más recae sobre la falta de conocimiento del tema.

Figura 1: Diagrama de Ishikawa



Fuente: Elaboración propia

Problema principal

¿En qué medida la implementación de un centro de operaciones de seguridad (SOC), incide en la detección de ataques cibernéticos en empresas del sector tecnológico?

Problemas secundarios

¿En qué medida el tipo de amenazas cibernéticas sofisticadas, influyen en los controles de seguridad de las organizaciones?

¿En qué medida la cantidad de recursos económicos influyen en el nivel de detección y contención de ataques cibernéticos?

¿De qué manera el grado de ausencia de un centro de operaciones de seguridad (SOC), genera un riesgo crítico para las organizaciones?

¿De qué manera el grado de conocimiento, influye en el porcentaje de contrarrestación de las amenazas cibernéticas?

Objetivo principal

Implementar un centro de operaciones de seguridad (SOC), que incida en la detección de ataques cibernéticos en empresas del sector tecnológico.

Objetivos secundarios

Determinar si el tipo de amenazas cibernéticas sofisticadas influyen en los controles de seguridad de las organizaciones

Analizar si la cantidad de recursos económicos influyen en el nivel de detección y contención de ataques cibernéticos.

Determinar si el grado de ausencia de un centro de operaciones de seguridad (SOC), genera un riesgo crítico para las organizaciones.

Evaluar si el grado de conocimiento, influye en el porcentaje de contrarrestación de las amenazas cibernéticas.

Definición de términos básicos

Centro de operaciones de ciberseguridad (SOC)

En seguridad informática el término centro de operaciones de seguridad, más conocido por su abreviación SOC es un área que implementan los equipos y/o especialistas de seguridad en las organizaciones con el objetivo de monitorear, analizar, detectar y responder a cualquier evento e incidente de seguridad que pudiese poner en riesgo la información y/u operaciones del negocio.

Muy independiente de las exigencias regulatorias que se exigen en el país, toda empresa mediana que utiliza activos tecnológicos debe implementar un centro de operaciones de seguridad (SOC) con el objetivo de poder identificar rápidamente las brechas de seguridad para tener acción rápida de contención y respuesta.

SIEM

El SIEM que por sus siglas significa (Security Information and Event Management) y traducido al español, Gestión de Eventos e Información de Seguridad es la herramienta core de todo centro de operaciones de seguridad (SOC) ya que mediante la misma se recopila toda la información de ocurrencias (logs) de cada herramienta que se desee monitorear, por ejemplo: Firewalls, switches, consolas de antivirus, consolas de IPS, consolas de antimalware, active directory, entre otros.

Así mismo la implementación de un SIEM, siempre va acompañado con la definición de una estrategia la cual debe contemplar el uso de la tecnología e infraestructura de manera óptima y adecuada.

Ataques cibernéticos

Un ataque cibernético hoy en día es muy conocido debido al auge en el cual se encuentra a nivel mundial y nacional, básicamente de lo que se trata es de un conjunto de acciones y secuencias pensadas y planificadas por una o más personas para aprovechar las debilidades de los activos tecnológicos inclusive el factor humano con el objetivo de lucrar a su conveniencia, bien puede ser haciendo uso de los recursos de tecnológicos, extorsión al negocio, extorsión a las personas afectadas, entre otros.

Los escenarios de ataques cibernéticos más conocidos hoy en día por su propagación son los siguientes:

- Ransomware
- Malware
- Phishing
- Fuga de información
- Ingeniería Social
- Ataques de día 0 (Zero-day)
- Denegación de servicios
- Amenazas persistentes avanzadas (ATP)
- Ataques web
- Man in the Middle

- Spoofing
- BEC (Business Email Compromise)

Seguridad informática

La Seguridad Informática o también llamada Ciberseguridad es un concepto muy difundido en la actualidad debido a la gran demanda de su adopción y utilización, indiferentemente de que nombre se utilice el objetivo siempre va a ser el mismo "Proteger la información que se almacena y transita mediante los activos tecnológicos".

La seguridad informática cubre 03 áreas principales respecto a la protección de información, la famosa triada CIA, a continuación, se detallan:

- **Confidencialidad (Confidentiality):** Asegurar la confidencialidad de los recursos de la compañía aplicando controles que permitan detectar y prevenir la fuga de información.

- **Integridad (Integrity):** Asegurar que la información no sea manipulada por terceros e inclusive internos no autorizados.

- **Disponibilidad (Available):** Asegurar la disponibilidad de la información para los usuarios que la consumen.

Marcos de trabajo y normas de ciberseguridad

NIST

El marco de Ciberseguridad del Instituto Nacional de Estándares y Tecnología (NIST) es un departamento que existe en los Estados Unidos los cuales se encargan de promover la elaboración y aprobación de estándares el cual sirva de apoyo para que los negocios puedan tener mayor entendimiento de los riesgos que trae consigo la Seguridad Informática.

El NIST se compone en las siguientes áreas: Identify, Protect, Detect, Response and Recovery.

- **Identificación (Identify):** El primer paso es identificar los activos dentro de la operación del negocio, tales como la lista de equipos que usan los usuarios, los programas que se le instalan, entre otros. Sumado a ello debe existir políticas que cubran las responsabilidades de los empleados, terceros y aquel que tenga acceso a información sensible.

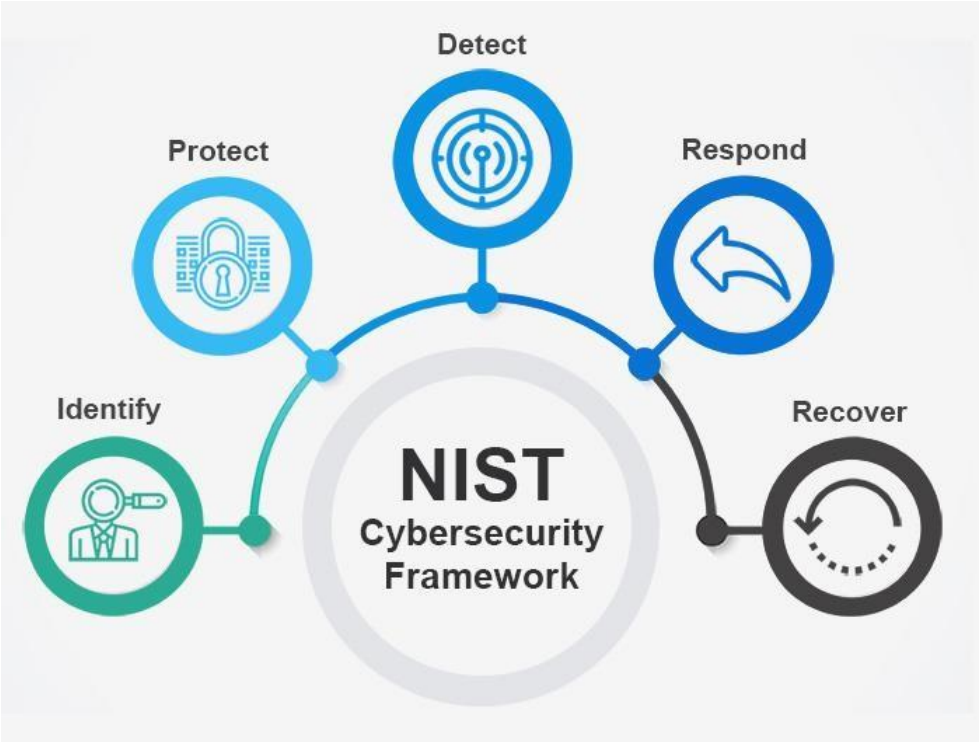
- **Protección (Protect):** Luego de identificar los activos ya podemos implementar herramientas y controles que sirvan de barrera (protección) para todo aquel usuario que no se encuentre autorizado y tenga malas intenciones. En esta área también se definen estrategias de respaldar la información como medida preventiva y proactiva ante un evento de no contención por la herramienta y/o control.

- **Detección (Detect):** Como siguiente paso luego de aplicar la protección se debe monitorear los activos para identificar de manera temprana los sucesos de mayor relevancia dentro de la red o dentro del servidor y/o cualquier otro involucrado.

- **Respuesta (Response):** La respuesta necesita del input de detección, de acuerdo con el análisis realizado por el factor humano, herramienta u otro, se gatilla una respuesta de contención ante cualquier escenario de ciberataque identificado.

- **Recuperación (Recovery):** Después de un escenario de ciberataque, se repara y restaura la operación de los equipos afectados.

Figura 2: Framework NIST CSF



ISO/IEC/ 270035

Con el objetivo de aportar en la gran variedad y cantidad ataques cibernéticos surge la normal internacional publicada por la ISO, lo cual se enfoca en guiar con buenas prácticas a los equipos de Seguridad Informática para una adecuada gestión de incidentes.

La ISO 27035 compone 04 pilares como base lo cual prepara a los equipos de Seguridad a gestionar de manera óptima y eficaz un incidente.

- **Preparación (Preparation):** Se definen las actividades base para la respuesta ante la materialización de un algún incidente de ciberseguridad.

- **Detección y Análisis (Detect & Analysis):** Detectar los eventos (logs) de seguridad aplicando una lógica definida en la cual consista categorizar el incidente según el escenario.

- **Contención, Erradicación y Recuperación (Content, Erradication & Recovery):** Son las actividades detalladas para controlar el incidente de seguridad para evitar la propagación; así mismo erradicar los procesos relacionados al incidente. Finalmente estar en la capacidad de recuperar los servicios ante una materialización que haya causa un daño grave.

- **Actividades de post incidente (Post Incident):** Son las lecciones aprendidas que deja el incidente con el fin de reforzar los puntos de control y optimizar el tiempo que se invierte en la gestión.

Justificación e importancia de la investigación

Hoy en día la importancia de realizar un trabajo de investigación sobre cómo afrontar las amenazas cibernéticas aporta mucho valor, ya que dentro este se identifica como las empresas de bajos recursos económicos no son conscientes de los riesgos de la exposición y muchas veces de manera inconsciente.

Justificación teórica

Se justifica implementar un centro de operaciones de ciberseguridad (SOC) con el objetivo de tener visibilidad de todos los eventos de las herramientas tecnológicas implementas en las empresas de TI, para ser más eficaces en la detección de amenazas cibernéticas para luego realizar un análisis y establecer una contención de estas para evitar daños.

Justificación empresarial

Las empresas que adopten esta propuesta se verán beneficiadas con la implementación de controles de seguridad y estrategias que le permitan tener mayor visibilidad de los sucesos por cada segundo dentro de su infraestructura tecnológica.

Los recursos económicos no son una limitante para la implementación de controles de ciberseguridad, por lo tanto, se justifica que cualquier empresa, desde chica, mediana y grande puede usar esta propuesta e implementarla.

Los riesgos críticos siempre van a existir en cualquier organización y más aún en Seguridad Informática que impacte directamente con el activo tecnológico, por lo tanto, también se justifica que la implementación de un centro de operaciones de ciberseguridad (SOC) reduce el riesgo en gran medida a las organizaciones que lo implementen.

Justificación social

El efecto de esta implementación tiene un grado beneficencia alto para la sociedad ya que el mismo sirve para cualquier empresa que quiera hacerles frente a los riesgos de las amenazas cibernéticas continuas, y no solamente se puede usar empresas, también se puede utilizar como referencia para realizar pruebas de simulación y aprendizaje en el área.

Conclusiones

La investigación comprobó que toda empresa que usa tecnología debe implementar al menos un centro de operaciones de ciberseguridad (SOC) el cual mejoró significativamente en la detección y respuesta de ataques cibernéticos, también aportó a la reducción de riesgos desde bajos, medios y críticos evitando así sufrir una amenaza sofisticada el cual pase a mayores.

El monitoreo y análisis brindó una visibilidad profunda de lo que sucedía con la operación de la tecnología y el comportamiento de los sistemas del negocio, contar con dichas actividades reforzó las capacidades de detección e identificación de los posibles escenarios de ataque, la misma que también permitió conocer cómo operan los ciberdelincuentes y que tanto conocen del rubro y la organización.

La parte económica fue una necesidad básica para la implementación; sin embargo, la misma no fue obstáculo para el centro de operaciones de ciberseguridad (SOC) ya que al tratarse de herramientas de costo 0 aportó enormemente a la necesidad.

Con lo implementado, las organizaciones fueron capaces de cerrar importantes brechas de seguridad que se identificaron directamente en tecnologías y en procesos de gestión, por lo tanto, la consideración de Seguridad Informática en las organizaciones aportó mucho aprendizaje y reforzó el grado madurez y cultura del país.

Aportes de la investigación

Ante la falta de cultura de Ciberseguridad en el País y el factor económico, se desarrolló la presente investigación de implementación de un SOC con el objetivo de garantizar la visibilidad de amenazas en las organizaciones y así reducir el número de empresas que no se preocupen por contrarrestar las amenazas de hoy en día en el Perú. La misma tomó como base estas dos importantes premisas en las cuales se pretende especificar y detallar.

La implementación de un centro de operaciones de ciberseguridad (SOC) mejoró la detección de ciberataques en empresas que no tengan una correcta definición del proceso, también mejoró el flujo de gestión de incidentes ya que este es uno de los pilares fundamentales que requieren pulir las organizaciones de cara a poder tener una óptima respuesta en un momento crítico.

Sumado a ello se minimizó el nivel de compromiso de ataques cibernéticos que en la actualidad casi no se toma en cuenta y no se es consciente de la gravedad de la situación, la misma permitirá aprender del proceso de gestión diario y retroalimentarse de manera continua.

Recomendaciones

Ejecutar un servicio de Hunting, es decir un proceso inicial de explotación de información de eventos (logs) para determinar el mayor punto de dolor que afecta y se debe monitorear y cubrir.

Implementar casos de uso basados en la detección de los comportamientos inusuales en las tecnologías implementadas a raíz de un Hunting, así como también considerando las buenas prácticas recomendadas por cada solución (marca).

Implementar un mantenimiento semestral de casos de uso y revisiones constantes de actualizaciones de las herramientas de seguridad informática que se utilizan como base para este proceso.

Desplegar una política en la cual se especifique que toda nueva herramienta tecnológica implementada se anexe al correlacionar de eventos (logs) y se diseñe un caso de uso para monitorear su comportamiento.

Ejecutar pruebas de efectividad por cada caso de uso implementado con el objetivo de poder validar si el mismo está diseñado de manera correcta y aporta valor al proceso.

Ejecutar pruebas periódicas de Ethical Hacking con el objetivo de identificar brechas de seguridad que deben cubrirse y tener al día.

Referencias

AMBIT (2020), *SOC: Que es y como implementarlo en tu empresa* https://www.ambit-bst.com/blog/soc-qu%C3%A9-es-y-c%C3%B3mo-implantarlo-en-tu-empresa

Diario Gestión (2021), *Perú sufrió más de 28 millones de ataques informáticos el 2020* https://gestion.pe/tecnologia/kaspersky-peru-sufrio-mas-de-28-millones-de-ataques-informaticos-el-2020-noticia

Encriptia (2017), *Security Operations Center (SOC)* https://encriptia.com/soc

EY (2021), *Ataques cibernéticos en Perú* https://www.ey.com/es_pe/news/2021/10/empresas-peruanas-preocupacion-ataques-ciberseguridad

ESAN (2019), *¿Qué es el Cybersecurity Framework de NIST de los Estados Unidos?* https://www.esan.edu.pe/conexion-esan/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos

INCIBE (2019), *Despliegue de SIEM en entornos TO* https://www.incibe-cert.es/blog/despliegue-siem-entornos

ISACA (2019), *Roles de las tres líneas de defensa para la seguridad de la información y gobierno* https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-4/roles-of-three-lines-of-defense-for-information-security-and-governance

INCIBE (2018), *Respondiendo a incidentes industriales SOC OT*. https://www.incibe-cert.es/blog/respondiendo-incidentes-industriales-soc-ot

ISACA (2018), *Arquitectura de Seguridad de la información*

https://www.isaca.org/es-es/resources/isaca-journal/issues/2018/volume-2/information-security-architecture-gap-assessment-and-prioritization

LinkedIn, Casanova (2020), *Construyendo un SOC con herramientas Open Source* https://es.linkedin.com/pulse/construyendo-un-soc-con-herramientas-open-source-i-aliaga-casanova

Márquez (2020). *Diseño de un Security Operations Center (SOC*). Universidad Politécnica Salesiana, Quito – Ecuador. Recuperado de https://dspace.ups.edu.ec/handle/123456789/18939

Mendoza y Vega (2019), *Evaluación de capacidades de detección y respuesta de un SOC*. Universidad del Pacífico, Lima – Perú. Recuperado de http://hdl.handle.net/11354/2250

NIST (1901), *Acerca de NIST* https://www.nist.gov/about-nist

NIST (2012), *Computer Security Incident Handling Guide* https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

PMG-SSI (2020), *ISO/IEC 27035: Gestión de incidentes de Seguridad* https://www.pmg-ssi.com/2020/07/iso-iec-27035-gestion-de-incidentes-de-seguridad

Rodríguez (2020). *Implementación de las operaciones y la gestión de un SOC*. Universidad Oberta de Catalunya, España. Recuperado de http://hdl.handle.net/10609/116526

Wikipedia (2021), *Ciberataques* https://es.wikipedia.org/wiki/Ciberataque

We Live Security (2015), *¿Ciberseguridad o Seguridad de la información? Aclarando la diferencia.*

https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/

Wikipedia (2020), *The MITRE Corporation*
https://es.wikipedia.org/wiki/The_MITRE_Corporation

Yolanda Corral (2020), *Construye y gestiona un SOC con herramientas Open Source*
https://www.yolandacorral.com/construye-y-gestiona-un-soc-con-herramientas-open-source/