AF 13.5 ARTÍCULO DE DIVULGACIÓN CIENTÍFICA.

LA INTEGRACIÓN DE LA CIBERINTELIGENCIA Y LA CIBERSEGURIDAD: UN FACTOR MULTIPLICADOR.

DEPARTAMENTO DE INTELIGENCIA.

Comandante D. Sergio NAVARRO LANGA.

12 de septiembre de 2025

ESCUELA SUPERIOR DE LAS FUERZAS ARMADAS

PÁGINA INTENCIONADAMENTE EN BLANCO

LA INTEGRACIÓN DE LA CIBERINTELIGENCIA Y LA CIBERSEGURIDAD: UN FACTOR MULTIPLICADOR.

Comandante de Artillería del ET. D. Sergio NAVARRO LANGA.

RESUMEN.

La ciberseguridad actual se enfrenta a adversarios cada vez más sofisticados, capaces de aprovechar vulnerabilidades en sistemas, cadenas de suministro o procesos humanos. Ante este panorama, reaccionar de manera improvisada ya no basta, se requiere método, modelos y operaciones integradas. Este artículo propone un marco práctico para lograrlo, combinando cuatro piezas ampliamente reconocidas, el ciclo de ciberinteligencia, el Modelo Diamante, la Cyber Kill Chain y la taxonomía MITRE ATT&CK.

El ciclo de ciberinteligencia proporciona el rumbo, define requisitos alineados con riesgos de negocio, organiza la recolección de datos, los procesa y analiza para transformarlos en inteligencia, difunde recomendaciones claras y retroalimenta el sistema con métricas verificables. El Modelo Diamante ofrece palancas inmediatas, recordando que cualquier intrusión conecta a un adversario, una víctima, una infraestructura y una capacidad, y que actuar sobre cualquiera de estos vértices encarece y dificulta la operación del atacante. La Cyber Kill Chain, por su parte, traza un eje temporal con ventanas de interrupción, cuanto antes se corte, más eficaz y menos costosa será la defensa. Finalmente, MITRE ATT&CK da el idioma común para detecciones, emulación y evaluación.

La integración de estos marcos se materializa en plataformas SIEM y SOAR, que permiten ver, entender y actuar. Se pasa del dato crudo a la alerta contextualizada, y de la alerta a la respuesta automatizada y repetible.

El lector encontrará aquí no solo un mapa conceptual, sino una invitación a transformar la ciberinteligencia en valor tangible, aprendiendo de casos reales y aplicando métricas que importan.

ABSTRACT.

Today’s cybersecurity faces increasingly sophisticated adversaries, capable of exploiting vulnerabilities in systems, supply chains, or human processes. In this landscape, improvisation is no longer enough: method, models, and integrated operations are required. This article proposes a practical framework to achieve that integration, combining four widely recognized elements: the Cyber

Intelligence Cycle, the Diamond Model, the Cyber Kill Chain, and the MITRE ATT&CK taxonomy.

The Cyber Intelligence Cycle provides direction: it defines requirements aligned with business risks, organizes data collection, processes and analyzes it to transform it into actionable intelligence, disseminates clear recommendations, and feeds the system back with measurable metrics. The Diamond Model offers immediate levers, reminding us that every intrusion connects an adversary, a victim, an infrastructure, and a capability, and that acting on any of these vertices increases the attacker's costs. The Cyber Kill Chain, in turn, provides a temporal axis with interruption windows: the earlier the cut, the more effective and less costly the defense. Finally, MITRE ATT&CK provides the common language for detection, emulation, and evaluation.

The integration of these frameworks materializes in SIEM and SOAR platforms, which allow organizations to see, understand, and act: from raw data to contextualized alerts, and from alerts to automated, repeatable responses.

The reader will find here not only a conceptual map, but also an invitation to transform cyber intelligence into tangible value, by learning from real cases and applying metrics that truly matter.

PALABRAS CLAVE.

Modelo Diamante, Cyber Kill Chain, MITRE ATT&CK, SIEM, SOAR.

KEY WORDS.

Diamond Model, Cyber Kill Chain, MITRE ATT&CK, SIEM, SOAR.

1. INTRODUCCIÓN.

MOTIVACIÓN, ALCANCE Y PRINCIPIOS DE DISEÑO.

La ciberseguridad moderna frente a intrusiones exige método, modelos y operativa. El método evita la reacción ad-hoc y convierte preguntas claves[1] en acciones verificables; los modelos estructuran la observación y ordenan las decisiones; mientras que la operativa o los artefactos operativos cierran el círculo

[1] Las preguntas clave son las preguntas que una organización necesita responder para orientar la toma de decisiones estratégicas, operacionales y/o tácticas.

en forma de reglas, *playbooks*[2], controles y métricas. En este artículo se integra cuatro piezas ampliamente aceptadas:

1. Ciclo de ciberinteligencia. Ciclo formado por seis fases. Dirección y Planificación → Recolección → Procesamiento → Análisis y Producción → Difusión. La última fase del ciclo es la Evaluación y Retroalimentación, fase trasversal a las otras cinco.
2. Modelo Diamante. Una intrusión puede analizarse y mitigarse manipulando cuatro vértices a modo de diamante (Adversario, Víctima, Capacidad e Infraestructura). Tocar y actuar en cualquiera de los vértices alteraría la acción del atacante.
3. Cyber Kill Chain (CKC). Es una secuencia teórica de un ciberataque que está compuesta por siete fases temporales (Reconocimiento, Preparación, Entrega, Explotación, Instalación, C2 y Acciones). Estas fases pueden indican ventanas de interrupción para cortar el ciberataque (cuanto antes, mejor).
4. MITRE ATT&CK. Es una taxonomía de tácticas (objetivos del adversario) y técnicas (métodos) por plataforma, con data sources, mitigaciones, grupos y software. Se puede decir que es el "idioma operativo" para detecciones, emulación y verificación.

La integración que se propone consiste en alinear preguntas clave con ventanas de interrupción del ciberataque (Cyber Kill Chain), escoger cuatro vértices realistas (Modelo Diamante), expresarlo con TTP´s normalizadas (ATT&CK) e introducirlo en plataformas SIEM[3] (ingesta, normalización, enriquecimiento y observabilidad) y SOAR[4] (orquestación y automatización). Este enfoque se apoya en documentación primaria como es la Cyber Kill Chain (Lockheed Martin, 2011), el desarrollo del Modelo Diamante (Caltagirone y otros, 2013), la base de conocimiento ATT&CK (MITRE ATT&CK, s.f.), y guías NIST[5].

---

[2] Los playbook de respuesta son documentos que detallan procedimientos y acciones a seguir por un equipo de respuesta ante incidentes de ciberseguridad. Estos guías estandarizan las respuestas a incidentes específicos, asegurando una acción rápida y coordinada para mitigar amenazas y reducir el impacto en la organización (Microsoft, 2024).

[3] SIEM: (Security Information and Event Managemen). Un SIEM es una plataforma que centraliza, normaliza y analiza los eventos de seguridad (logs) de toda la organización.

[4] SOAR: (Security Orchestration, Automation and Response). Un SOAR es una plataforma que conecta detección con acción.

[5] NIST: (National Institute of Standards and Technology). Instituto Nacional de Estándares y Tecnología de los Estados Unidos.

2. EXPOSICIÓN.

2.1. LOS CUATRO MARCOS.

2.1.1. Ciclo de ciberinteligencia.

El ciclo de ciberinteligencia es un procedimiento repetible que evita la deriva reactiva. Formula requisitos claros alineados con la organización; planifica y prioriza fuentes de alto valor; procesa y analiza para reconstruir el hilo causal; difunde recomendaciones accionables con responsables y fechas; y retroalimenta el sistema con métricas y lecciones aprendidas. En la práctica, cada secuencia repetitiva debe obtener productos y herramientas (reglas versionadas, *playbooks*, cambios de configuración, bloqueos con TTL[6], documentación de evidencias) y medidas métricas (MTTD/MTTC/MTTR[7], precisión de reglas y porcentajes de cortes tempranos).

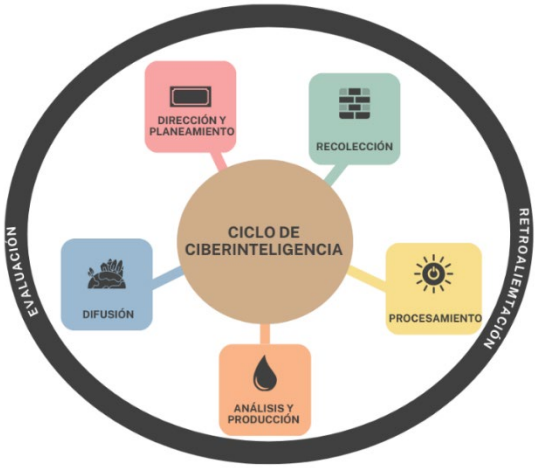

Figura 1. Ciclo de ciberinteligencia. Fuente de elaboración propia.

Dirección y Planeamiento.

Es la fase estratégica del ciclo. Aquí se definen los requisitos de inteligencia, es decir, qué se quiere saber, para qué y en qué plazo.

---

[6] TTL: (Time To Live). Es un valor en segundos o en “saltos” que llevan los paquetes IP en su cabecera.

[7] MTTD: (Mean Time To Detect). Tiempo medio que tarda un equipo en detectar un incidente. MTTC: (Mean Time To Contain). Tiempo medio en contener un incidente una vez detectado. MTTR: (Mean Time To Recover). Tiempo medio para recuperar sistemas tras un incidente.

Los requisitos deben estar alineados con los riesgos de la organización (por ejemplo, reducir en un 70% el fraude por cambio de cuentas bancarias en seis meses). Se deben de establecer prioridades (qué amenazas importan más, qué vectores son críticos, y en qué puntos de la Cyber Kill Chain conviene interrumpir). Se finaliza esta fase con el producto esperado, un plan de inteligencia con objetivos, alcance y métricas.

Recolección.

En esta fase se obtienen los datos necesarios para responder a los requisitos definidos en la fase de Dirección y Planeamiento.

Las fuentes típicas para obtener información son: correo (detección de spear phishing); DNS/HTTP (análisis de dominios y tráfico web); IdP/AD[8] (eventos de autenticación), EDR/NDR[9] (telemetría de endpoints y red); y Cloud control plane y servicios SaaS[10] críticos.

Es recomendable definir los campos mínimos obligatorios y una política de retención sostenible.

El principio clave de esta fase es la priorización. Priority logs[11] (no todos los logs valen lo mismo; priorizar los que generan más inteligencia útil).

Procesamiento.

Aquí los datos crudos se convierten en información estructurada y comprensible. Y para ello se debe normalizar fechas y zonas horarias; usar parsers[12] para extraer campos relevantes; evitar duplicidades; y enriquecer con etiquetas la

[8] IdP: (Identity Provider). Servicio que gestiona y autentica identidades digitales en entornos corporativos o en la nube. AD (Active Directory): Directorio de Microsoft usado para gestionar usuarios, grupos y recursos en redes empresariales.

[9] EDR: (Endpoint Detection and Response). Solución de seguridad para monitorizar y responder a amenazas en dispositivos finales. NDR (Network Detection and Response): Tecnología que detecta amenazas analizando tráfico de red.

[10] SaaS: (Software as a Service). Modelo de distribución de software en la nube bajo suscripción.

[11] Logs: Son registros cronológicos y detallados de todo lo que pasa en un dispositivo, aplicación, red o servicio de los sistemas informáticos.

[12] Un parser (analizador) es como el “traductor automático” entre datos crudos y datos estructurados y comprensibles.

información (como determinar en qué fase de la CKC ocurre el ciberataque, táctica/técnica ATT&CK, criticidad del activo, tipo de identidad).

Análisis y producción.

Esta fase está dividida en dos sub-fases.

Por un lado, la sub-fase de Análisis en la que se debe de correlacionar eventos para reconstruir hilos causales (no solo coincidencias de campos); detectar patrones de comportamiento, pivotando con el Modelo Diamante; e identificar anomalías relevantes frente a falsos positivos.

Por otro lado, se encuentra la sub-fase de Producción donde se obtiene el producto esperado. Entre los productos destacan las reglas de detección versionadas, listas negras o blancas con TTL definido, controles de proceso, playbooks para SOAR con pasos claros y reversibles.

Es importante que cada producto venga identificado con el responsable designado de la producción y la fecha de revisión.

Difusión.

La inteligencia ya procesada se transforma en acciones verificables que llegan a los clientes adecuados.

El objetivo de esta fase es que la inteligencia no quede en informes, sino en cambios operativos concretos. Y para ello debe de llegar al cliente adecuado (need-to-share).

Evaluación y Retroalimentación.

Esta fase es trasversal al resto, cerrando el ciclo y garantizando la mejora continua.

Se evalúan resultados: métricas de tiempo: MTTD, MTTC, MTTR (con percentiles); calidad (F1[13] de reglas críticas); porcentaje de cortes tempranos en la Kill Chain; resiliencia (RTO/RPO[14] ensayados); si las métricas no mejoran, se

[13] F1 (F1 Score): Métrica de precisión en detección que combina recall y precision.

[14] RTO (Recovery Time Objective): Es el tiempo máximo tolerable que un servicio puede estar caído tras un incidente antes de que afecte gravemente al negocio**.** RPO (Recovery Point Objective): Es la cantidad máxima de datos que se puede perder, medida en tiempo. Dicho de otra forma: el “punto en el tiempo” al que los sistemas deben restaurarse.

replantean fuentes de obtención, requisitos o acciones; y todo se debe documentar como lecciones aprendidas para la siguiente iteración.

2.1.2. Modelo Diamante.

El Modelo Diamante es un método desarrollado por (Caltagirone y otros, 2013) que formaliza todo evento de intrusión conectando cuatro atributos: Adversario, Víctima, Capacidad e Infraestructura. Estos atributos se conectan por relaciones invariantes (por ejemplo, Capacidad ↔ Infraestructura y Adversario ↔ Capacidad) y permiten pivotar entre vértices para descubrir actividad relacionada (hilos de actividad, campañas). La fortaleza del modelo está en que, interaccionando sobre cualquier vértice, se obtiene una acción sobre el adversario.

Unidad de análisis. El "evento". Un evento es la mínima interacción observable del adversario. Los eventos se encadenan en hilos de actividad (misma infraestructura, misma capacidad, mismas horas) y, a su vez, componen campañas (misión/objetivo consistente). Registrar metadatos del evento (hora, entorno, fuente, mapeo ATT&CK, fase CKC) permite construir grafos explotables de forma computacional.

Invariantes analíticas. Se destacan relaciones constantes (por ejemplo, Adversario–Capacidad[15]: un actor tiende a reutilizar o evolucionar un malware o exploit; Capacidad–Infraestructura: una técnica requiere rutas específicas ,…). Estas invariantes guían detección por comportamiento y priorizan controles, es decidir, qué medidas defensivas aplicar primero en función del impacto esperado (qué daño evita), de la probabilidad de la amenaza (qué tan probable es que ocurra) y del coste/beneficio (qué tan caro o difícil es implementar una medida y cuánto reduce el riesgo).

[15] La invariante analítica Adversario-Capacidad es muy importante y utilizada ya que el adversario suele reutilizar, adaptar o evolucionar sus capacidades técnicas, así como reflejar un patrón estable en el tiempo debido a que la herramienta está vinculada al actor, incluso cuando cambia la víctima o el escenario.

Errores comunes.

Existen una serie de errores fáciles de cometer como es el obsesionarse con la atribución temprana (buscar lo antes posible el nombre del actor) en lugar de tocar Infraestructura/Capacidad, que es una invariante analítica. Además de no versionar diamantes por incidente (de esta manera se pierde trazabilidad) y fijar bloqueos “eternos” (se debe de usar TTL, revisar los indicadores y definir TTP si se encuentra patrón).

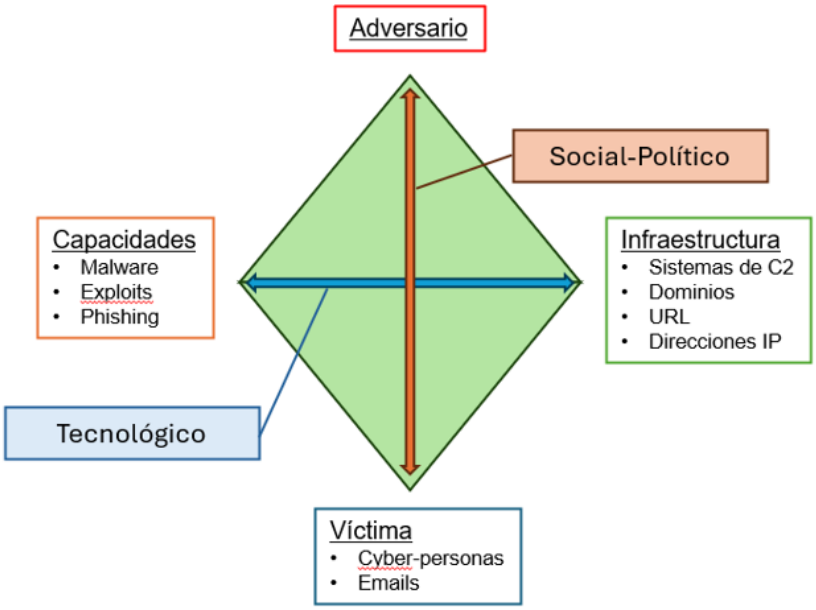

Figura 2. Modelo Diamante. Fuente de elaboración propia.

2.1.3. Cyber Kill Chain.

La Cyber Kill Chain (CKC) de Lockheed Martin estructura la actividad adversaria en siete fases que, más que una receta lineal, constituyen un mapa temporal de oportunidades de defensa ante el ciberataque. Cada fase admite controles preventivos y reactivos, y su valor práctico reside en que interrumpir de manera temprana es menos costoso y más eficaz (cuanto antes, mejor).

Fases y medidas defensivas.

Reconocimiento. En esta fase inicial, el atacante lleva a cabo reconocimiento y obtención de información sobre el objetivo. Es difícil detectar al adversario en esta fase, pero las organizaciones pueden reducir el riesgo realizando control del expuesto, higiene de metadatos y reducción de superficie de ataque (deshabilitar plugins innecesarios).

Preparación. El atacante prepara su arma maliciosa específica para inyectarla en el objetivo. Se debe de evitar recolección masiva de información y realizar una configuración de infraestructura maliciosa.

Entrega. Fase en la que el atacante inyecta el arma maliciosa en el sistema víctima. Para evitarlo se pueden tomar las siguientes medidas: correo (filtros), web (proxy, URL filtering), detección de dominios look-alike[16] y URL acortadas.

Explotación. Fase en la que el atacante gana la entrada el sistema de la víctima. Se aconseja impedir ejecución de macros no firmadas y usar anti-exploit.

Instalación. Si la explotación tuvo éxito, el atacante podría proceder a instalar malware persistente en el sistema de la víctima. Se puede usar autoruns vigilados, control de aplicaciones y EDR con bloqueos.

C2. En esta etapa, el atacante obtiene control remoto sobre la máquina comprometida. Para evitarlo se puede realizar detecciones de beaconing[17], o inspecciones de protocolos.

Acciones. Es la fase final de la cadena, donde el adversario ejecuta sus últimas acciones dentro del sistema víctima para conseguir sus objetivos finales. Una vez alcanzado el objetivo final en una víctima, el atacante puede repetir el ciclo contra nuevos objetivos / victimas. Se recomienda disponer de Kill-switch operativo (aislar host/segmento) y RTO/RPO ensayados.

Errores comunes.

Es muy importante evitar cometer errores comunes como puede ser el tratar la CKC como un checklist rígido o colocar sensores sólo al final. La solución pasa por pensar en ventanas de oportunidad para romper el ataque en el caso de una CKC rígida y en el caso del segundo error, reforzar las fases de Entrega / Explotación / Instalación.

[16] Un dominio look-alike es un dominio falso creado para parecerse al legítimo, con el objetivo de engañar a usuarios o sistemas.

[17] El beaconing es un patrón de comunicación típico del malware y de las infraestructuras de C2.

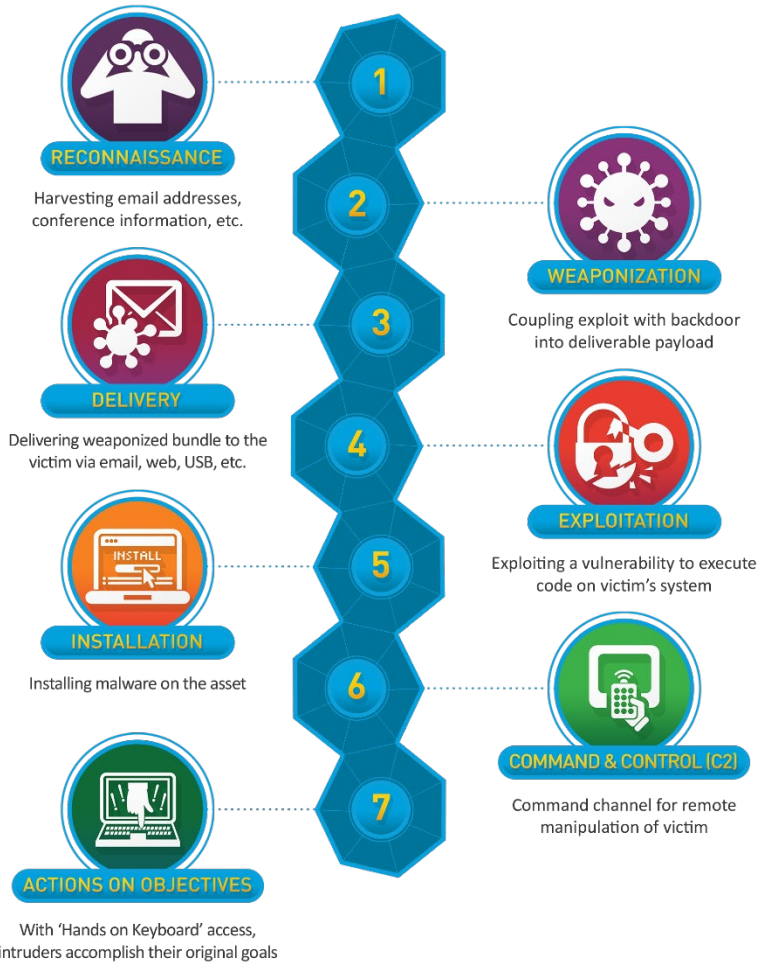

Figura 3. Diagrama de las siete fases de la Cyber Kill Chain. Fuente (Lockheed Martin, 2011).

2.1.4. MITRE ATT&CK.

ATT&CK[18] es una base de conocimiento viva, basada en análisis y que organiza tácticas (el "por qué") y técnicas (el "cómo") por plataforma (Windows, macOS, Linux, etc.). Además, proporciona software, data sources/components, mitigaciones y relaciones. Es el "idioma común" para detección, hunting, emulación y evaluación.

Diseño de detecciones centradas en TTP.

El diseño de detecciones centradas en TTP exige mapear cada regla con su correspondiente táctica y técnica del marco ATT&CK, seleccionando fuentes de

[18] Matriz ATT&CK.

datos apropiadas (como *Process Creation (Windows)* para la técnica T1059 o *Network Flow* para T1071) y desarrollando lógicas que permitan identificar patrones de comportamiento en los ataques, superando la limitada eficacia de las reglas basadas únicamente en IoC. Este enfoque requiere, además, validar las detecciones mediante la emulación en entornos controlados de las mismas tácticas o técnicas utilizadas por adversarios reales, de modo que sea posible capturar evidencias operativas (alertas, tickets, medidas de contención) y medir métricas clave como MTTD o MTTC por TTP. Finalmente, la cobertura defensiva debe documentarse y revisarse de manera sistemática utilizando herramientas como ATT&CK Navigator, que facilitan la visualización del grado de protección alcanzado en distintas plataformas y servicios.

Priorización. No es aconsejable intentar "cubrirlo todo". Es mejor seleccionar 10/15 técnicas prioritarias por plataforma según las amenazas probables, la exposición e el impacto (por ejemplo, T1566 Phishing, T1204 User Execution, T1059 Command/Scripting). Se debe de renovar la lista trimestralmente con base en incidentes y threat intel.

Citas y fuentes, no opiniones: ATT&CK aporta definiciones y ejemplos que evitan discusiones semánticas, facilitan auditorías y permiten comparar coberturas entre equipos y periodos.

Errores comunes.

Entre los errores más habituales en la aplicación de este modelo se encuentra el uso de ATT&CK como una simple lista de verificación, lo que genera una sobrecarga en el equipo de seguridad. La solución pasa por establecer una adecuada priorización y verificación de técnicas.

Otro error recurrente es no vincular las reglas de detección con componentes de datos específicos, ya que no basta con afirmar que una regla detecta una técnica de ATT&CK. Es imprescindible definir qué "data components" permiten esa detección, diseñando las reglas con los datos en mente.

Finalmente, la emulación sin registro de evidencias impide mantener la trazabilidad del proceso, dificultando demostrar qué técnica se probó, qué falló o qué funcionó. La forma de resolverlo es adoptar un enfoque de detections-as-code, documentando, versionando y probando cada detección con herramientas que respalden su eficacia y permitan su auditoría.

2.2. PLATAFORMAS SIEM / SOAR.

2.2.1. SIEM. Ojos, memoria y contexto.

El SIEM (Security Information and Event Management) es la plataforma central de observación en la que se materializa la integración de los modelos teóricos con la operación. No es solo un recolector de logs, es como el radar del SOC[19], el que traduce datos crudos en eventos comprensibles y comparables.

2.2.2. SOAR. Orquestación y automatización.

El SOAR (Security Orchestration, Automation and Response) es el brazo ejecutor de la integración. Si el SIEM “ve y entiende”, el SOAR “actúa y cierra”. Es la torre de control que emite órdenes rápidas y seguras a partir de la información contextualizada que recibe.

2.3. INTEGRACION DE LOS CUATRO MARCOS. CICLO DE CIBERINTELIGENCIA, MODELO DIAMANTE, CYBER KILL CHAIN Y MITRE ATT&CK.

La arquitectura de integración es la relación entre análisis (ciberinteligencia) y respuesta (ciberseguridad):

El **ciclo de ciberinteligencia** define qué preguntas responder, qué señales capturar y cómo medir.

El **Modelo Diamante** ofrece acciones defensivas inmediatas y de alto impacto que derivan de los vértices del diamante establecido (Infraestructura/Capacidad/Víctima/Adversario).

La **CKC** da el eje temporal (ventanas de interrupción) y prioriza la ubicación de sensores para romper el ciberataque.

ATT&CK convierte todo en detections-as-code, emulación y evidencias con nombres normalizados.

[19] SOC: (Security Operations Center). Es el equipo o unidad que se encarga de monitorizar, detectar, analizar y responder a incidentes de ciberseguridad en una organización.

2.4. FUNCIÓN DE SIEM Y SOAR EN LA INTEGRACIÓN.

2.4.1. Función e impacto directo del SIEM en la integración.

Función SIEM en la integración.

El SIEM normaliza y enriquece los eventos, ya que unifica formatos, etiqueta incidentes (fase CKC, táctica/técnica ATT&CK, vértice del Diamante) y resuelve identidades/activos. Además, permite que los marcos analíticos (CKC, ATT&CK, Modelo Diamante y ciclo de ciberinteliogencia) hablen un mismo idioma en cada alerta. También, actúa como punto de unión semántico, cada evento tiene contexto temporal (CKC), técnico (ATT&CK), estratégico (Diamante) y metodológico (ciclo).

Impacto directo del SIEM en la integración.

Sin SIEM, los modelos quedarían en el plano teórico; con SIEM, se transforman en alertas accionables.

Los casos reales que se verán a continuación lo demuestran. En WannaCry, la disponibilidad de telemetría SMB[20] en el SIEM y su mapeo a ATT&CK (T1210) permitió identificar actividad maliciosa temprana. Donde no hubo SIEM ni telemetría contextualizada, la integración no existió.

El SIEM es como el radar de un aeropuerto. Sin radar, los aviones vuelan, pero la torre de control no puede interpretarlos ni dirigirlos.

2.4.2. Función e impacto directo del SOAR en la integración.

Función del SOAR en la integración.

El SOAR toma la alerta ya etiquetada (CKC, ATT&CK, Diamante) y ejecuta un playbook predefinido, que podría ser aislar un host, bloquear un dominio con TTL o suspender una cuenta, entre otras. Por otro lado, conecta detección (SIEM) con acción inmediata (contención/mitigación) y finalmente, cierra el ciclo de ciberinteligencia retroalimentando reglas y controles ya que cada acción deja evidencia, tiempos medidos y lecciones aprendidas.

[20] La telemetría SMB hace referencia a los datos de registro y observación que generan las comunicaciones realizadas a través del protocolo SMB (Server Message Block), muy utilizado en Windows para compartir archivos, impresoras y otros recursos en red.

Impacto directo del SOAR en la integración.

El empleo de un SOAR reduce el MTTC (Mean Time to Contain), una métrica crítica en ciberdefensa integrada; y asegura que la respuesta sea coherente y repetible, no depende del azar ni de la rapidez de un analista.

Casos como Emotet, que se verán posteriormente, muestran su valor al detectar un correo malicioso (fase CKC: Entrega, técnica ATT&CK: T1566), ya que un SOAR bien configurado podría cuarentenar el correo, bloquear el dominio por 7 días y notificar al usuario en minutos de manera automática, sin clics manuales.

Siguiendo la metáfora del SIEM, el SOAR es como la torre de control del aeropuerto: recibe el radar (SIEM), interpreta las cartas de navegación (modelos) y ejecuta órdenes rápidas y coordinadas (bloquear, desviar, aislar).

2.5. INDICADORES QUE IMPORTAN. GOBERNANZA DE MÉTRICAS Y VERIFICACIÓN.

La efectividad de un programa de ciberseguridad no puede evaluarse únicamente por la existencia de controles, sino por la capacidad de medir su desempeño de manera objetiva, verificable y alineada con los riesgos reales. Para ello, resulta esencial definir un conjunto de indicadores que permitan valorar tiempos de detección y respuesta, calidad de las reglas implementadas, madurez del programa de registros y nivel de resiliencia operativa. Entre los más importantes destacan los tiempos medios (MTTD, MTTC y MTTR, medidos con percentiles), el porcentaje de cortes tempranos en fases iniciales del ataque (Entrega, Explotación o Instalación frente a fases posteriores como C2 o Acciones), la calidad de las detecciones expresada en métricas como el F1 de las reglas críticas, la observabilidad del programa de logging mediante un plan estructurado de recopilación, almacenamiento y gestión de eventos; y finalmente, la resiliencia comprobada a través de pruebas y ensayos de RTO y RPO.

Por otro lado, señalar que se deben de diseñar métricas reproducibles y que cambien decisiones; que se alineen con NIST SP 800-92/92r1, SP 800-137 y las guías CISA/ACSC 2025 (incluida Priority Logs).

2.6. CASOS REALES EXPLICADOS CON CICLO, DIAMANTE, KILL CHAIN Y ATT&CK.

2.6.1. WannaCry (2017). Cuando un parche atrasado cuesta millones.

Qué pasó. Un ransomware se extendió por el mundo aprovechando una vulnerabilidad antigua de Windows (SMBv1). Un analista registró un dominio incrustado que actuó como "kill switch" y frenó la propagación; además, aplicar el parche MS17-010 cerraba la puerta usada por el gusano.

Lectura con nuestros modelos.

- CKC. La Entrega/Explotación aprovechan SMBv1; y la Infraestructura incluye el dominio de "kill switch". Por lo que cortar ahí ralentizó el ataque global.
- Diamante. Accionando el vértice Infraestructura (dominio de control) y el de Capacidad (parchear SMBv1, deshabilitarlo) se redujo el daño drásticamente.
- ATT&CK. Técnicas de movimiento y explotación traducidas a reglas en SIEM/EDR.

Qué funcionó.

- Parcheo de MS17-010 (priorizado), deshabilitar SMBv1 donde era innecesario y segmentar redes.
- Bloquear el dominio "kill switch" en redes internas para detectar y aislar equipos que lo consultaban (señal de infección).
- Copias de seguridad verificadas para recuperar. Resiliencia.

Lección. Medir y priorizar vulnerabilidades para establecer parches críticos; y mantener telemetría y alertas casi en tiempo real (conexiones anómalas SMB, consultas a dominios raros).

2.6.2. SolarWinds (2020). El caballo de Troya en las actualizaciones.

Qué pasó. Una actualización de un software muy usado venía "envenenada", abriendo una puerta discreta a miles de clientes. Decisores ordenaron desconectar versiones afectadas e iniciar análisis forense. Se emitieron directivas y guías para contener y erradicar el ciberataque.

Lectura con nuestros modelos.

- Diamante. Capacidad (backdoor en actualización), Infraestructura (servidores de control), Víctimas (clientes Orion).
- CKC. La fase de Entrega fue la propia actualización; la de C2 fue discreto y de baja señal. Cortar en la fase de C2 (bloqueos de salida, listas "allow") y desconectar fue clave en la resolución del ciberincidente.
- ATT&CK. Técnicas de persistencia y exfiltración mapeadas para detecciones específicas.

Qué funcionó.

- Desconexión inmediata del software afectado y verificación de integridad.
- Bloqueos de comunicaciones salientes no justificadas y revisión de credenciales.
- Revisión de la cadena de suministro (listas blancas de dependencias/actualizaciones y monitoreo de egress[21]).

Lección. El eslabón débil puede ser un proveedor. Por eso, conviene medir "salidas" no habituales y validar actualizaciones críticas antes de desplegarlas masivamente.

2.6.3. Colonial Pipeline (2021). Cuando el ransomware apaga un país.

Qué pasó. El grupo DarkSide desplegó ransomware en los sistemas de TI de Colonial Pipeline, lo que obligó a detener operaciones críticas de suministro de combustible en EE. UU.

Lectura con nuestros modelos.

- Diamante. Víctima (operador de infraestructura crítica), Capacidad (encryptor de DarkSide), Infraestructura (red de pago de rescates).
- CKC**.** Acceso inicial mediante credenciales comprometidas, Acciones→ cifrado de datos.
- ATT&CK. T1078 (Valid Accounts), T1486 (Encrypt for Impact).

[21] Egress. Es el tráfico de salida desde una red interna hacia el exterior.

Qué funcionó.

- Segmentación entre entornos TI/OT.
- Respuesta del FBI y recuperación parcial del rescate en criptomonedas.
- Refuerzo de controles de identidad.

Lección. La identidad es el nuevo perímetro. Sin MFA[22] ni gestión robusta de cuentas, incluso las infraestructuras críticas pueden paralizarse.

2.6.4. Emotet (2021). Cuando la "infraestructura del adversario" cae.

Qué pasó. Una operación coordinada internacional (Europol + FBI + varios países) tomó el control de la infraestructura del botnet Emotet y lo desmanteló temporalmente. Es el clásico caso de derrotar al adversario tocando el vértice Infraestructura del diamante.

Lectura con nuestros modelos.

- Diamante. Cortar Infraestructura obliga al adversario a reconstruir su operativa, lo que le conlleva subir sus costes.
- CKC. Se dificulta C2 y redistribución del ataque en otros sistemas (fase de Acción).
- ATT&CK. Reglas de detección de beacons y listas negras dinámicas.

Qué funcionó.

- Cooperación policial y técnica, sinkholing y toma de control.
- En las empresas, bloquear dominios/IPs comprometidos, rotar credenciales y revisar persistencias.

Lección. La inteligencia compartida y actuable es una palanca enorme; por eso un TIP[23] y estándares como STIX/TAXII[24] son esenciales.

---

[22] MFA: (Multi-Factor Authentication). Es un mecanismo de autenticación que exige más de un factor para verificar la identidad de un usuario.

[23] TIP: (Threat Intelligence Platform). Es una plataforma de inteligencia de amenazas diseñada para centralizar, procesar y operacionalizar la información sobre ciberamenazas.

[24] STIX/TAXII: STIX (Structured Threat Information eXpression), TAXII (Trusted Automated eXchange of Indicator Information). Son dos estándares complementarios que se usan para compartir inteligencia de ciberamenazas de manera estructurada y automatizada.

3. CONCLUSIONES.

Integración como engranaje entre modelos y operaciones.

La integración de marcos analíticos y operativos funciona como un engranaje que conecta el plano de la inteligencia con la ejecución técnica. El ciclo de ciberinteligencia establece las preguntas clave y define las métricas que orientan el esfuerzo analítico, mientras que el Modelo Diamante proporciona palancas inmediatas de defensa a través de sus vértices —Infraestructura, Capacidad, Víctima y Adversario—, permitiendo identificar puntos críticos de intervención. Por su parte, la Cyber Kill Chain introduce el eje temporal que ayuda a localizar las ventanas de interrupción a lo largo del ciclo de vida del ataque. A este conjunto se suma MITRE ATT&CK, que aporta un lenguaje común y normalizado para describir detecciones, emulación y evidencias.

Integrar estos marcos no es un ejercicio teórico. Significa que cada evento que ingresa en el SIEM puede ser traducido, correlacionado y respondido en el SOAR bajo una semántica compartida, asegurando coherencia entre la inteligencia producida y la defensa aplicada.

SIEM y SOAR como motores de la integración.

El SIEM no se limita a almacenar registros, sino que los normaliza y enriquece, de modo que cada alerta generada incluye su correspondencia con una fase de la Cyber Kill Chain, la táctica o técnica de ATT&CK asociada y el vértice relevante del Modelo Diamante.

El SOAR, por su parte, transforma esa detección en acción, garantizando una respuesta de contención rápida, repetible y trazable.

En conjunto, ambas plataformas materializan la integración en la práctica, permitiendo no solo ver y entender los eventos, sino también actuar de manera coordinada y eficaz frente a las amenazas.

Métricas que sí importan.

Las métricas clave para evaluar la eficacia de un programa de ciberseguridad incluyen el MTTD (tiempo medio de detección), el MTTC (tiempo medio de contención) y el MTTR (tiempo medio de recuperación), siempre medidos en percentiles para reflejar mejor la variabilidad de los casos. A ello se suma el porcentaje de cortes tempranos, que mide la capacidad de interrumpir el ataque en fases iniciales de la CKC como Entrega, Explotación o Instalación, en lugar de permitir que avance hasta etapas críticas de C2 o Acciones. La calidad de las detecciones también debe evaluarse, utilizando para ello métricas como el F1 de las reglas críticas. Finalmente, la observabilidad del programa de logging,

entendida como la capacidad de recopilar, almacenar y explotar datos relevantes, constituye un pilar esencial.

En conjunto, estas métricas orientan la inversión de seguridad de manera más efectiva que el simple conteo de alertas generadas.

Lecciones de casos reales.

- WannaCry mostró la importancia de parches y segmentación temprana.
- SolarWinds confirmaron el riesgo sistémico de la cadena de suministro.
- Colonial Pipeline evidenció que la identidad es el nuevo perímetro.
- Emotet demostró la potencia de tocar Infraestructura mediante cooperación internacional.

Síntesis final.

La defensa eficaz no depende sólo de más herramientas, sino de alinear método (ciclo de ciberinteligencia), modelos (Modelo Diamante, Cyber Kill Chain, MITRE ATT&CK) y operaciones (SIEM, SOAR). Integrar significa:

- Ver antes, gracias a telemetría normalizada.
- Cortar antes, actuando en fases tempranas.
- Aprender siempre, transformando incidentes en cambios permanentes.

En resumen, la integración práctica de los cuatro marcos en SIEM y SOAR, junto con métricas verificables, es lo que convierte la ciberinteligencia en un valor tangible y multiplicador para la ciberseguridad.

(4456)

NAVARRO LANGA SERGIO - 72974859E

Firmado digitalmente por NAVARRO LANGA SERGIO - 72974859E
Fecha: 2025.09.12 09:42:34 +02'00'

PÁGINA INTENCIONADAMENTE EN BLANCO

BIBLIOGRAFÍA

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.

Cybersecurity and Infrastructure Security Agency. (2017, 1 de julio). Petya Ransomware.https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware.

Cybersecurity and Infrastructure Security Agency. (2020, 13 de diciembre). ED 21-01: Mitigate SolarWinds Orion Code Compromise. https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise.

Cybersecurity and Infrastructure Security Agency. (2021, 23 de diciembre). Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (AA21-356A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2021, 6 de julio). Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack. https://www.cisa.gov/news-events/alerts/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa-supply-chain-ransomware-attack.

Dempsey, K. (2011). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137.

Dempsey, K. (2020). Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment (NIST SP 800-137A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137A.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Hutchins, M. (2017, 13 de mayo). How to Accidentally Stop a Global Cyber Attack. MalwareTech Blog. https://malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

Microsoft. (2017, 14 de marzo). Microsoft Security Bulletin MS17-010 – Critical: Security Update for Microsoft Windows SMB Server (4013389). https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010.

Caltagirone, S., Pendergast, A., & Betz, C. (2013). The Diamond Model of Intrusion Analysis. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf.

Cybersecurity and Infrastructure Security Agency. (2017, 1 de julio). Petya Ransomware.https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware.

Cybersecurity and Infrastructure Security Agency. (2020, 13 de diciembre). ED 21-01: Mitigate SolarWinds Orion Code Compromise. https://www.cisa.gov/news-events/directives/ed-21-01-mitigate-solarwinds-orion-code-compromise.

Cybersecurity and Infrastructure Security Agency. (2021, 23 de diciembre). Mitigating Log4Shell and Other Log4j-Related Vulnerabilities (AA21-356A). https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-356a.

Cybersecurity and Infrastructure Security Agency & Federal Bureau of Investigation. (2021, 6 de julio). Guidance for MSPs and their Customers Affected by the Kaseya VSA Supply-Chain Ransomware Attack. https://www.cisa.gov/news-events/alerts/2021/07/04/cisa-fbi-guidance-msps-and-their-customers-affected-kaseya-vsa-supply-chain-ransomware-attack.

Dempsey, K. (2011). Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations (NIST SP 800-137). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137.

Dempsey, K. (2020). Assessing Information Security Continuous Monitoring (ISCM) Programs: Developing an ISCM Program Assessment (NIST SP 800-137A). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-137A.

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin. https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.

Hutchins, M. (2017, 13 de mayo). How to Accidentally Stop a Global Cyber Attack. MalwareTech Blog. https://malwaretech.com/2017/05/how-to-accidentally-stop-a-global-cyber-attacks.html.

Microsoft. (2017, 14 de marzo). Microsoft Security Bulletin MS17-010 – Critical: Security Update for Microsoft Windows SMB Server (4013389). https://learn.microsoft.com/es-es/security-updates/securitybulletins/2017/ms17-010.

MITRE Corporation. (s. f.). Enterprise Matrix — MITRE ATT&CK®. (Consulta: 3 de septiembre de 2025). https://attack.mitre.org/matrices/enterprise/.

Scarfone, K. A., & Souppaya, M. (2023). Cybersecurity Log Management Planning Guide (NIST SP 800-92 Rev. 1, Initial Public Draft). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-92r1.ipd.

Strom, B. E., Applebaum, A., Miller, D. P., Nickels, K. C., Pennington, A., & Thomas, C. B. (2020). MITRE ATT&CK®: Design and Philosophy (rev. de 2018). MITRE. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf.

U.S. Department of Justice. (2021, 7 de junio). Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to Ransomware Extortionists DarkSide [Comunicado de prensa]. https://www.justice.gov/archives/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside.

U.S. Department of Homeland Security, Cyber Safety Review Board. (2022, 11 de julio). Review of the December 2021 Log4j Event. https://www.cisa.gov/sites/default/files/2023-02/CSRB-Report-on-Log4j-PublicReport-July-11-2022-508-Compliant.pdf.

United States Government. (2025, abril). Computer Security Incident Handling: Recommendations and Considerations for Cyber Risk Management (NIST SP 800-61, Rev. 3). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-61r3.

World’s most dangerous malware EMOTET disrupted through global action. (2021, 27/28 de enero). Europol [Nota de prensa]. https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action