

ESTUDIO DE REFERENCIA SOBRE PLATAFORMAS DE CIBERSEGURIDAD PARA CSIRTS ACADÉMICOS

*Un estudio de EU CyberNet y la LAC4 realizado Koen van Impe & Carlos Leonardo
2025*



Prefacio

EU CyberNet y el Centro de Ciber capacidades de Latinoamérica el Caribe (LAC4) elaboraron el Estudio de Referencia sobre Plataformas de Ciberseguridad, diseñado específicamente para Equipos de Respuesta a Incidentes Cibernéticos (CSIRT) Académicos. Este exhaustivo trabajo aborda una necesidad crítica y creciente en la región de LAC: dotar a las instituciones académicas de soluciones de ciberseguridad robustas, escalables y rentables para defenderse eficazmente de una gama cambiante de amenazas cibernéticas.

El panorama digital en América Latina y el Caribe se caracteriza por una gran diversidad de infraestructura, disponibilidad de recursos y experiencia técnica. A medida que los CSIRT académicos se enfrentan a amenazas como ataques DDoS, malware, accesos no autorizados y filtraciones de datos, es fundamental seleccionar las herramientas de ciberseguridad adecuadas. Este estudio proporciona una guía esencial al evaluar un amplio espectro de plataformas comerciales y de código abierto, lo que garantiza que las instituciones académicas puedan tomar decisiones informadas que se adapten mejor a sus entornos operativos y limitaciones presupuestarias.

La importancia estratégica de este trabajo radica no solo en su utilidad inmediata para fortalecer la postura de seguridad de las instituciones académicas, sino también en el fomento de una cultura de ciberseguridad sostenible en toda la región. Al destacar soluciones que combinan funcionalidad, escalabilidad, capacidades de integración y rentabilidad, este estudio permite a los CSIRT académicos mejorar sus capacidades, compartir conocimientos de forma más eficaz y colaborar de forma proactiva para abordar los desafíos de la ciberseguridad.

EU CyberNet y LAC4 creen que la ciberseguridad es una responsabilidad compartida y que el desarrollo de capacidades a nivel académico sienta las bases para una mayor resiliencia regional. Mediante esfuerzos colaborativos como este estudio de referencia, nos comprometemos a promover un entorno digital seguro y resiliente, apoyar a la comunidad académica y, en última instancia, fortalecer el ecosistema de ciberseguridad en toda América Latina y el Caribe.

Expresamos nuestro más profundo agradecimiento a todos los colaboradores y partes interesadas, cuya experiencia y perspectivas han hecho posible este estudio y lo han hecho tan impactante. Esperamos que este trabajo sea un recurso valioso para las instituciones académicas que se esfuerzan por proteger a sus comunidades y contribuir positivamente a la resiliencia regional en materia de ciberseguridad.

César Moliné Rodríguez

Director Regional

Tabla de contenido

Prefacio	2
Tabla de contenido	3
1. Introducción	4
Contexto	4
Metodología	5
Consulta a las partes interesadas	5
Cronograma	6
Contribuyentes	6
Madurez de CSIRT	6
2. Revisión de literatura e investigación documental	7
Introducción	7
Investigación	8
Soluciones de ciberseguridad	8
SIEM	8
DDOS	9
WAF	9
Herramientas de hacking ético	9
Servicios y plataformas de inteligencia sobre amenazas cibernéticas	10
3. Consulta a partes interesadas	11
Introducción	11
Metodología	11
Hallazgos	12
Soluciones de código abierto o comerciales	12
Soporte y escalabilidad	13
Intercambio en la comunidad	13
Flexibilidad en la elección	13
Licencias	13
SIEMs	13
DDoS / WAF	14
Herramientas de hacking ético	14
Servicios y plataformas de CTI	14
Resultados de la encuesta	15
4. Conclusiones	17
SIEM	17
DDOS and WAF	17
Herramientas de hacking ético	18
Servicios y plataformas de inteligencia de amenazas cibernéticas	18
Consideraciones para la implementación	19
Limitaciones y trabajos futuros	19
5. Apéndice	19
Apéndice 1. Metodología - criterios de evaluación detallados	19
Apéndice 2. Preguntas de entrevista	20
Apéndice 3. Preguntas de encuesta	23

1. Introducción

Contexto

El panorama de la ciberseguridad evoluciona rápidamente y presenta importantes desafíos para los **Equipos de Respuesta ante Incidentes de Seguridad Informática (CSIRTs) en el ámbito académico**. Estos equipos tienen la tarea de proteger a las instituciones académicas frente a una amplia variedad de amenazas, incluyendo ataques de denegación de servicio distribuido (DDoS), accesos no autorizados, malware y filtraciones de datos. Para abordar eficazmente estos desafíos, los CSIRTs requieren plataformas de ciberseguridad sólidas, escalables y rentables, adaptadas a sus necesidades operativas específicas.

La diversidad de soluciones de ciberseguridad disponibles, que abarca desde sistemas de Gestión de Información y Eventos de Seguridad (SIEM), cortafuegos para aplicaciones web (WAF), herramientas de mitigación de ataques DDoS, plataformas de hacking ético y servicios y plataformas de Inteligencia de Amenazas Cibernéticas (CTI), exige una evaluación exhaustiva que sirva de guía para la toma de decisiones sobre adquisición e implementación. Este estudio comparativo tiene como objetivo identificar, comparar y evaluar tanto soluciones comerciales como de código abierto para apoyar a los CSIRTs académicos en el fortalecimiento de su postura de ciberseguridad.

Los objetivos principales de este estudio comparativo son:

1. **Identificación de soluciones:** Catalogar plataformas de ciberseguridad existentes que aborden áreas clave como SIEM, protección DDoS, WAF, herramientas de hacking ético y servicios y plataformas de CTI.
2. **Análisis comparativo:** Evaluar las plataformas identificadas con base en criterios predefinidos, tales como funcionalidad, escalabilidad, facilidad de uso, capacidades de integración, costo y soporte del proveedor.
3. **Recomendaciones estratégicas:** Proporcionar recomendaciones fundamentadas a los CSIRTs académicos para seleccionar e implementar las plataformas de ciberseguridad más adecuadas.
4. **Desarrollo de capacidades:** Dotar a los CSIRTs académicos de conocimientos y perspectivas que les permitan tomar decisiones informadas en materia tecnológica.

Metodología

El estudio comparativo adoptó un enfoque en múltiples fases:



1. **Revisión de literatura:** Realizar una revisión de publicaciones académicas y de la industria para identificar las principales soluciones de ciberseguridad y tendencias relevantes para los CSIRT académicos.
2. **Consulta a partes interesadas:** Organizar consultas con CSIRT académicos y expertos del sector para recopilar requisitos y prioridades.
3. **Identificación de soluciones:** Compilar una lista de plataformas potenciales basadas en investigación de mercado y aportes de las partes interesadas.
4. **Desarrollo del marco de evaluación:** Diseñar un marco de evaluación con criterios ponderados para valorar las soluciones.
5. **Pruebas y análisis de plataformas:** Realizar pruebas prácticas (cuando sea posible) y analizar materiales proporcionados por los proveedores, estudios de caso y reseñas.
6. **Elaboración del informe:** Sintetizar los hallazgos en un informe integral con recomendaciones prácticas.

Consulta a las partes interesadas

Como parte del proceso de consulta a las partes interesadas, se llevaron a cabo entrevistas¹ con profesionales experimentados en ciberseguridad de las comunidades CSIRT y CSIRT académicas, así como una encuesta entre actores clave en la región objetivo. Sus valiosos aportes sirvieron como base para este estudio. En particular, nos gustaría expresar nuestro agradecimiento a:

- **Sam Foster**
- **Marco Gallardo**
- **George Giorgakis**
- **Michael S Kun**
- **Andre R. Landim**
- **Jorge Merchan**
- **Thomas Schreck**

¹Las solicitudes de retroalimentación por parte de las partes interesadas se compartieron a través de la lista de correo y el canal de Slack de FIRST.org, LinkedIn y grupos privados de Signal. Además, estas solicitudes fueron difundidas a través de diversos grupos académicos y de investigación por miembros de la comunidad FIRST.

Cronograma

Este estudio se llevó a cabo en 2025, más específicamente:

- Febrero, marzo y abril de 2025: Revisión de literatura y consultas a las partes interesadas.
- Marzo y abril de 2025: Identificación de soluciones y desarrollo del marco de evaluación.
- Abril y mayo de 2025: Pruebas y análisis de plataformas, preparación y difusión del informe.

Contribuyentes

Este estudio fue realizado por **Koen Van Impe** and **Carlos Leonardo**.

Madurez de CSIRT

Este estudio proporciona principalmente insumos para que los CSIRTs mejoren los parámetros del Cuadrante de "Herramientas" del estándar de madurez SIM3².

Este cuadrante se refiere al conjunto de programas, aplicaciones, servicios, instrumentos e incluso equipos simples utilizados por el CSIRT para alcanzar sus objetivos y ofrecer los servicios necesarios. El cuadrante contiene los siguientes parámetros relevantes:



- T-1 Activos y configuraciones de TI
- T-2 Lista de fuentes de información
- T-3 Sistema(s) de mensajería consolidado(s)
- T-4 Sistema de seguimiento de incidentes
- T-5 Llamadas de voz resilientes
- T-6 Mensajería resiliente
- T-8 Conjunto de herramientas para la prevención de incidentes
- T-9 Conjunto de herramientas para la detección de incidentes
- T-10 Conjunto de herramientas para la resolución de incidentes

El estudio proporciona principalmente insumos para la prevención (T8), detección (T9) y resolución (T10) de incidentes.

² Gestión de Incidentes de Seguridad - <https://opencsirt.org/csirt-maturity/sim3-and-references/>

2. Revisión de literatura e investigación documental

Introducción

Aunque la cantidad de herramientas de ciberseguridad disponibles para los CSIRTs es extensa, las soluciones específicamente diseñadas para CSIRTs académicos³ siguen siendo relativamente limitadas. Esto no resulta sorprendente, dado que estos equipos enfrentan una amplia variedad de amenazas en **entornos heterogéneos** y deben apoyarse en tecnologías diversas para la prevención, detección, análisis y respuesta. Como ocurre con muchos aspectos de los CSIRTs (y de los SOCs), no existe⁴ una solución única para todos los casos; distintos equipos priorizarán diferentes herramientas según sus flujos de trabajo particulares. No obstante, como mínimo, un CSIRT requiere su propia **infraestructura dedicada**, que le permita operar de forma independiente de la unidad tecnológica general.

Y aunque muchas plataformas prometen una vista centralizada tipo “ventana única” (single pane of glass), en la práctica esto rara vez se cumple. En su lugar, el enfoque más eficaz es contar con herramientas diseñadas para propósitos específicos que aseguren una fuerte integración entre ellas. Esta estrategia funciona mejor cuando se combina con **automatización** de tareas repetitivas, escalamiento ágil y una **gestión eficiente de incidentes**.

Los CSIRTs académicos también enfrentan desafíos⁵ distintos a los de las estructuras corporativas típicas, reflejando a menudo su enfoque orientado a la investigación. Los presupuestos pueden ser limitados, y se suele preferir el uso de herramientas de código abierto⁶ para mantener la flexibilidad y reducir costos, lo que en algunos casos lleva a la creación de CSIRTs⁷ completamente basados en herramientas open source. Aun así, la selección de herramientas suele depender de la capacidad local, la formación disponible y de cómo se dividen las responsabilidades de seguridad entre los equipos de TI centrales y departamentales.

Además, las redes académicas suelen operar con un ancho de banda significativamente mayor que muchos entornos empresariales, y alojan servicios diversos, a veces experimentales. Estos entornos de alto rendimiento y gran variabilidad pueden representar grandes desafíos a la hora de seleccionar y

³ Construyendo un equipo de seguridad en la academia: propuesta de un nuevo concepto - Martin Havránek, Václav Lohr, Pavel Ambruz, Martin Lukáš, Miloš Ulman - <https://ceur-ws.org/Vol-3857/paper10.pdf>

⁴ MTIRE - 11 Strategies of a world-class Cybersecurity Operations Center - <https://www.mitre.org/sites/default/files/2022-04/11-strategies-of-a-world-class-cybersecurity-operations-center.pdf>

⁵ Diseño de un CSIRT académico: una propuesta basada en principios de planificación estratégica - https://www.researchgate.net/publication/352270744_Design_of_an_academic_CSIRT_-_A_proposal_based_on_strategic_planning_principles

⁶ F&OSS Tools for CSIRTs by Josef Šmidrkal - <https://tf-csirt.org/wp-content/uploads/2022/09/smidrkal-67tfcirt-LT-FOSS-Tools-for-CSIRTs.pptx>

⁷ How to Build a CIRT based on Open source tools by Marwan BEN RACHE - https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Africa_Cyberdrill_18/Presentations/5-Services.pdf

mantener soluciones de seguridad, especialmente en lo que respecta a la mitigación de ataques DDoS y la monitorización a gran escala.

Investigación

Se ha publicado relativamente poca investigación centrada específicamente en soluciones de ciberseguridad para CSIRTs académicos. Una excepción notable es un informe de ENISA⁸ de 2020, *Detección proactiva: medidas y fuentes de información*, sobre métodos, herramientas, actividades y fuentes de información que los equipos europeos de respuesta a incidentes están utilizando o podrían utilizar para detectar incidentes de seguridad en la red. Aunque el repositorio de GitHub⁹ asociado no ha sido actualizado desde junio de 2020, el estudio sigue siendo un recurso valioso para los CSIRTs académicos que buscan orientación sobre herramientas de monitoreo de red y fuentes de inteligencia de amenazas. Un rastreador indicativo en el repositorio señala si un recurso en particular sigue activo, lo que ofrece un punto de referencia útil para los profesionales.

Además, el estudio *Design of an Academic CSIRT - A Proposal Based on Strategic Planning Principles* ofrece¹⁰ información¹¹ sobre las **razones para establecer un CSIRT académico** y describe los pasos clave del proceso. Aunque no se enfoca en la selección de herramientas de ciberseguridad, el estudio proporciona un marco estratégico para comprender por qué las instituciones académicas podrían crear un equipo de respuesta dedicado, haciendo hincapié en la estructura organizativa y en consideraciones de planificación a largo plazo.

Soluciones de ciberseguridad

SIEM

La elección de un sistema SIEM está estrechamente vinculada a la misión y los requisitos específicos de cada CSIRT académico. Si bien documentos como la *Guía del comprador de SIEM*¹² ofrecen criterios útiles de selección, muchas de esas pautas están dirigidas a entornos empresariales o comerciales, más que a los entornos de investigación distribuidos que se encuentran en el ámbito académico.

En la práctica, varios CSIRTs académicos dependen del conjunto de herramientas Elastic Stack para satisfacer sus necesidades de SIEM. Su flexibilidad lo hace adecuado no solo para la supervisión interna estándar, sino también para la ingestión de servicios e indicadores de amenazas, la monitorización de datos de honeypots y el análisis del tráfico de red en enlaces académicos de alto rendimiento. Variantes del Elastic Stack, como SecurityOnion¹³ y SOF-ELK¹⁴, cumplen funciones más especializadas: SecurityOnion combina¹⁵ monitoreo avanzado de seguridad con gestión de casos, mientras que SOF-ELK está

⁸ <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Report%20-%20Proactive%20detection%20-%20Measures%20and%20Information%20sources.pdf>

⁹ <https://github.com/enisaeu/IRtools>

¹⁰ https://www.researchgate.net/publication/358338647_Design_of_an_Academic_CSIRT_-_A_Proposal_Based_on_Strategic_Planning_Principles

¹¹ <https://www.youtube.com/watch?v=dIO5ozWZIPY>

¹² SIEM Buyer's Guide - DomainTools - https://www.domaintools.com/wp-content/uploads/SIEM_Buyers_Guide.pdf

¹³ <https://securityonionsolutions.com/>

¹⁴ <https://www.sans.org/tools/sof-elk/>

¹⁵ ISOC Kazakhstan and cybersecurity challenge - https://2019.caigf.org/wp-content/uploads/2018/07/Nurlybaev_ISOC_KZ.pdf

diseñado para “análisis de big data” orientado a personal de operaciones de seguridad e informática forense. Es importante destacar que Elastic también admite la supervisión de endpoints. Sin embargo, ha habido ciertas preocupaciones respecto a los cambios en los modelos de licenciamiento de Elastic, lo que puede dificultar algunas implementaciones.

DDOS

Dado que muchas instituciones académicas operan redes comparables a las de pequeños o medianos proveedores de servicios de Internet, los ataques DDoS son una preocupación constante, especialmente en contextos políticos o sociales inestables donde puede aumentar la actividad hacktivista. Las soluciones comerciales a gran escala para mitigación de DDoS suelen ser costosas, lo que lleva a los CSIRTs académicos a buscar alternativas más ingeniosas.

En Europa, GÉANT (la colaboración de las Redes Nacionales de Investigación y Educación europeas) ofrece una herramienta de detección y análisis de DDoS llamada NeMo¹⁶, pero ofertas similares a gran escala aún no están fácilmente disponibles para instituciones de América Latina y el Caribe. Aunque existen servicios comerciales de protección contra DDoS en la región, la asequibilidad sigue siendo una barrera, y los CSIRTs en entornos académicos suelen compensar con una combinación de soluciones de limpieza de código abierto scrubbing, modelado y filtrado de tráfico local, y coordinación con redes nacionales de investigación.

WAF

En contextos empresariales generales, los WAF (Firewalls de Aplicaciones Web) suelen incluirse junto con herramientas de protección de endpoints. Sin embargo, en entornos académicos, el uso de WAFs varía. Algunos CSIRTs informan que la mitigación de DDoS y la monitorización general de la red son prioritarias, mientras que las soluciones WAF dedicadas se utilizan con menor frecuencia, a menos que la infraestructura web principal de la institución enfrente ataques dirigidos a nivel de capa de aplicación.

Además, la infraestructura web pública del CSIRT, o de su organización matriz, puede no ser un objetivo tan atractivo en comparación con la infraestructura web pública de los institutos académicos. Como resultado, el rol del CSIRT en la seguridad de aplicaciones web puede centrarse más en brindar asesoramiento que en operar un WAF independiente.

Herramientas de hacking ético

Las plataformas para el hacking ético **pueden variar significativamente dependiendo de cómo las organizaciones definan el término**. Algunas consideran que estas plataformas son herramientas estándar de gestión de vulnerabilidades, como Nessus¹⁷, mientras que otras incluyen soluciones de escaneo de paquetes y

¹⁶ <https://security.geant.org/nemo-ddos-software/>

¹⁷ <https://www.tenable.com/products/nessus>

redes (como ZMap y Nmap¹⁸) en esta categoría. También hay quienes consideran que marcos de explotación como Metasploit¹⁹ representan plataformas de “hacking ético”.

Independientemente de cómo se etiqueten las plataformas, comúnmente se reconocen como herramientas importantes para el aprendizaje y la formación, ya que ayudan a los equipos a comprender cómo se llevan a cabo los ataques y cómo detectarlos y defenderse de ellos de la mejor manera. Además de estas herramientas de prueba activa, vale la pena destacar la disponibilidad de conjuntos de datos proporcionados por **Team Cymru**²⁰ y **Shadowserver**²¹. Estos feeds a gran escala aportan un valor considerable a los CSIRTs académicos, especialmente a aquellos con capacidades de escaneo limitadas. Los equipos más maduros se benefician de estos conjuntos de datos externos para complementar su propia inteligencia y mejorar la visibilidad general de la red.

Servicios y plataformas de inteligencia sobre amenazas cibernéticas

Además de los conjuntos de datos de Team Cymru y Shadowserver, muchos CSIRTs académicos dependen de fuentes OSINT²² ampliamente disponibles, como Ransomlook²³ y Abuse.ch²⁴, para obtener inteligencia sobre amenazas valiosa²⁵. Estos canales pueden enriquecer la visibilidad local y proporcionar datos útiles e inmediatos sobre amenazas emergentes.

Las plataformas comerciales de inteligencia sobre amenazas suelen ser prohibitivamente caras para los equipos académicos, que por ello tienden a preferir soluciones de código abierto. Entre las más comunes se encuentran MISP, una plataforma consolidada para compartir y correlacionar inteligencia sobre amenazas, y OpenCTI, que ofrece un enfoque moderno para la ingestión y gestión de indicadores.

Algunos proveedores comerciales de servicios de inteligencia sobre amenazas también ofrecen servicios gratuitos limitados pero útiles. Por ejemplo, OTX AlienVault²⁶ proporciona acceso abierto a un amplio conjunto de indicadores de amenazas, mientras que VirusTotal ofrece una versión gratuita de su servicio de detección de malware y escaneo de archivos/dominios. De manera similar, URLScan también brinda un servicio gratuito para el análisis de URLs. Estos recursos pueden ser excelentes complementos para que los CSIRTs académicos amplíen su cobertura de amenazas sin incurrir en altos costos.

¹⁸ <https://nmap.org/>

¹⁹ <https://www.metasploit.com/>

²⁰ <https://www.team-cymru.com/>

²¹ <https://www.shadowserver.org/>

²² <https://github.com/hslatman/awesome-threat-intelligence>

²³ <https://www.ransomlook.io/>

²⁴ <https://abuse.ch/>

²⁵ Threat Intelligence for Research & Education by Roderick Mooi during <https://tf-csirt.org/wp-content/uploads/2022/05/22-05-11-TF-CSIRT-Threat-intelligence-for-Research-and-Education-RMooi.pdf>

²⁶ <https://otx.alienvault.com/>

3.Consulta a partes interesadas

Introducción

Entre febrero y abril de 2025, se llevaron a cabo una serie de **entrevistas** con partes interesadas clave, la mayoría de las cuales desempeñan un papel activo en la selección y adquisición de herramientas de ciberseguridad, o trabajan estrechamente con colegas que lo hacen. Estas entrevistas, que generalmente duraban alrededor de una hora, se realizaron principalmente en línea mediante videoconferencia, y se condujeron en inglés o en español.

Antes de cada entrevista, se proporcionó a los participantes un conjunto de preguntas preparadas (ver apéndice). Durante la entrevista, se les dio amplia oportunidad de hablar sobre sus experiencias y comentar sobre cualquier punto adicional. Aunque los participantes podían optar por ser mencionados como colaboradores del estudio, las respuestas individuales se mantendrán anónimas y no se atribuirán directamente a ningún entrevistado.

Como complemento a las entrevistas, se utilizó una **encuesta** para recopilar datos cuantitativos de partes interesadas clave, con un enfoque principal en la región de América Latina y el Caribe. Esta encuesta nos permitió validar y verificar los hallazgos obtenidos en las entrevistas.

En general, la mayoría de los participantes tenía experiencia práctica en el uso diario de las soluciones de ciberseguridad que discutieron, o había trabajado de cerca con los equipos operativos. En consecuencia, las observaciones de esta sección reflejan una perspectiva práctica sobre cómo se seleccionan, implementan e integran estas herramientas dentro de diversos entornos académicos de CSIRTs.

Metodología

Para el estudio, la escala de puntuación utilizada en el análisis comparativo se basa en una **matriz de evaluación del 1 al 5**, adaptada a los criterios más relevantes para los CSIRTs académicos, considerando la funcionalidad, escalabilidad, facilidad de uso, capacidades de integración, costo y soporte del proveedor.

- **1: Deficiente** - No cumple con los requisitos mínimos o presenta obstáculos graves.
- **2: Limitado** - Cumplimiento parcial, con deficiencias técnicas u operativas significativas.
- **3: Aceptable** - Funciona de manera adecuada, pero requiere ajustes o soporte adicional.
- **4: Bueno** - Cumple con la mayoría de los requisitos clave, con limitaciones menores.
- **5: Excelente** - Cumple o supera todas las expectativas sin limitaciones importantes.

Se encuestó a un grupo seleccionado de partes interesadas sobre estos criterios:



- **Funcionalidad:** Evalúa la amplitud y profundidad de las capacidades técnicas: detección de amenazas, análisis de comportamiento, automatización, cumplimiento normativo, generación de informes.
- **Integración:** Mide la facilidad para conectarse con otras herramientas (SIEM, WAF, registros, endpoints, APIs) y flujos de trabajo existentes.
- **Usabilidad:** Analiza la curva de aprendizaje, claridad de la interfaz, documentación, disponibilidad de capacitación y facilidad de implementación.
- **Escalabilidad:** Mide qué tan bien se adapta la solución a un entorno académico con eventos, usuarios o nodos en crecimiento.
- **Soporte y comunidad:** Evalúa el acceso a soporte técnico, mantenimiento, actualizaciones, foros, documentación y frecuencia de nuevas versiones.

En el apéndice se proporciona una visión general que vincula cada criterio con su puntuación.

Hallazgos

Soluciones de código abierto o comerciales

La mayoría de los entrevistados expresó una **clara preferencia por las soluciones de código abierto**. Algunos equipos comienzan con software de código abierto para desarrollar un caso de uso y establecer una gobernanza, migrando luego a una plataforma comercial una vez que los requerimientos y flujos de trabajo están más maduros. Otros equipos utilizan tanto soluciones de código abierto como comerciales de forma redundante, para lograr una mayor cobertura y visibilidad. La dependencia de herramientas de código abierto es aún más marcada en el caso de las utilidades de ethical hacking. Los CSIRTs las prefieren no solo por su flexibilidad y eficiencia en costos, sino también porque la experiencia práctica profundiza la comprensión de los analistas sobre técnicas de ataque y explotación de vulnerabilidades.

Una ventaja importante de las soluciones de código abierto que se destacó fueron sus capacidades y el sólido soporte para **integrarse** con otras herramientas. Este beneficio, sin embargo, suele requerir personal con experiencia para desplegar y mantener estos sistemas. Las posibilidades de integración también son un criterio clave en la selección de productos comerciales. La integración se centra principalmente en construir conectores personalizados o trabajar con automatización, a menudo mediante interacciones con APIs y scripting en Python.

Algunos CSIRTs incluso mantienen equipos técnicos dedicados para configurar funciones de integración para el CSIRT Académico.

Soporte y escalabilidad

En general, los actores involucrados se mostraron satisfechos con el **soporte de la comunidad** disponible para las soluciones de código abierto, aunque varios señalaron que navegar por los diferentes canales de soporte puede ser un desafío. Las contribuciones directas a los proyectos de código abierto siguen siendo limitadas; en cambio, algunos participantes optan por retribuir indirectamente comprando paquetes de soporte comercial ofrecidos por la comunidad cuando están disponibles. También se informó que el soporte por parte de proveedores comerciales ha sido sólido.

Los participantes indicaron que las soluciones escalan bien, aunque esto requiere la capacidad de agregar hardware (virtual) adicional para soportar más nodos o clústeres.

Intercambio en la comunidad

Muchas partes interesadas distribuyen habitualmente informes, alertas y eventos de amenazas del PSIM a sus grupos de interés. Sin embargo, también observaron que las limitaciones legales o técnicas a veces limitan el intercambio con una comunidad más amplia.

Flexibilidad en la elección

La mayoría de los participantes disfruta de una considerable libertad para seleccionar sus herramientas. La principal restricción es el presupuesto limitado con el que deben operar sus equipos.

Licencias

Para los productos con licencia, los participantes adoptan diversas estrategias de gestión de costos. Algunos optan por acuerdos plurianuales con precios fijos para mantener los gastos previsibles, mientras que otros prefieren licencias perpetuas para poder posponer actualizaciones pagadas o nuevas funciones hasta que haya presupuesto adicional disponible.

SIEMs

Los CSIRTs dependen de una combinación de SIEMs de código abierto y comerciales. **Splunk, Wazuh y Elastic** son los más ampliamente desplegados, mientras que **FortiSIEM, Graylog e IBM QRadar** aparecen en un número menor de entornos. Algunos equipos operan sin un SIEM dedicado.

La satisfacción general es alta: muchos CSIRTs han mantenido la misma plataforma durante seis años o más, lo cual es un testimonio tanto de su estabilidad como de su adecuación a los flujos de trabajo. Los CSIRTs informaron

que, en general, sus soluciones **cumplen con la mayoría de sus requerimientos clave**.

Varios participantes admitieron que no estaban aprovechando completamente las capacidades de su SIEM. Para reducir los costos de las soluciones comerciales, algunos consideran implementar un pipeline de filtrado antes del SIEM, eliminando eventos benignos o irrelevantes. La colaboración con los proveedores se centra en el trabajo de integración, la automatización y la reducción de falsos positivos.

DDoS / WAF

Los CSIRT académicos también están satisfechos con sus soluciones de mitigación de DDoS y protección WAF. La mayoría depende de servicios comerciales de proveedores como Akamai, Netscout (Arbor), Cloudflare, AWS, Radware o Fortinet, mientras que una minoría utiliza opciones de código abierto como ModSecurity. Al igual que con las plataformas SIEM, la satisfacción general es alta, los equipos han conservado estas soluciones durante muchos años y **satisfacen la mayoría de sus requisitos clave**.

Herramientas de hacking ético

Los CSIRT académicos dependen principalmente de herramientas de hacking ético de código abierto, que a menudo complementan con herramientas comerciales.

Su arsenal incluye utilidades "atómicas" como Metasploit, Burp Suite, Zap, Impacket y Pantera, junto con herramientas multipropósito como Kali Linux y escáneres de vulnerabilidades como Nessus y Greenbone (OpenVAS). Los participantes señalaron que estos escáneres pueden generar volúmenes abrumadores de datos, lo que requiere que los equipos dediquen un esfuerzo considerable a ajustar los flujos de trabajo y suprimir alertas benignas.

Los CSIRT académicos indicaron que estas herramientas son en su mayoría **aceptables**, aunque algunas de sus funciones requieren ajustes adicionales o soporte.

Servicios y plataformas de CTI

Los servicios y plataformas de inteligencia de amenazas cibernéticas (CTI) ocupan un rol estratégico para los CSIRT académicos entrevistados. Los equipos los utilizan primero como un **motor de concienciación**, para seguir los cambios en el panorama de amenazas y transmitir esa información a analistas y responsables. En la mayoría de los casos, los equipos están satisfechos con sus plataformas, ya que **cumplen con la mayoría de sus requisitos clave**.

La mayoría de los encuestados ha probado varias plataformas, pero tienden a establecerse en **MISP**, valorando sus amplias opciones de integración. Los participantes destacaron que el intercambio temprano, a través de la plataforma, API o distribución por correo electrónico –especialmente durante campañas de ransomware, puede ahorrar valiosas horas en detección y respuesta, y permite a los campus actuar de manera más proactiva.

Algunos equipos complementan **MISP** con OpenCTI y servicios comerciales como Zerofox, que elogian por sus datos confiables y soporte ágil, especialmente en el monitoreo de la red oscura, así como SOCRadar. Más allá de las plataformas, los feeds de amenazas universalmente disponibles de Team Cymru y Shadowserver, además del feed **MISP** de **FIRST**²⁷, se consideran indispensables; muchos entrevistados los describieron como las primeras fuentes externas que integran en cualquier canal de concienciación o notificación.

Resultados de la encuesta

Se diseñó y administró una encuesta estructurada a especialistas en ciberseguridad, ingeniería y tecnología de la información con experiencia en la implementación o evaluación de soluciones de ciberseguridad, específicamente en redes académicas de CSIRT. El instrumento evaluó seis dimensiones clave utilizando una escala Likert de 1 a 5.

La encuesta abarcó un conjunto amplio de herramientas en varias categorías: plataformas de SIEM y monitoreo como Wazuh, ELK Stack, ModSecurity, Splunk y QRadar; plataformas de inteligencia de amenazas como OpenCTI, MISP, SOCRadar, Recorded Future, Zerofox; y fuentes de amenazas como FIRST, Shadowserver y Team Cymru; herramientas de pruebas de penetración como Kali Linux, Metasploit Pro, Cobalt Strike y Burp Suite; y soluciones de mitigación de DDoS como Netscout (Arbor Networks), Radware, Cloudflare, AWS WAF y F5 WAF.

²⁷ <https://www.first.org/global/sigs/information-sharing/misp>

Solución	Plataforma	Funcionalidad	Integración	Usabilidad	Escalabilidad	Rentabilidad / Relación costo-beneficio	Soporte técnico
SIEM	Elastic (Comercial / Código abierto)	3.80	4.17	3.83	4.33	3.83	3.50
	Splunk (Comercial)	3.50	3.60	3.75	3.80	2.60	3.50
	QRadar (Comercial)	3.33	3.00	2.67	2.67	2.33	2.80
	Wazuh (Código abierto)	4.17	4.00	4.00	4.50	4.83	3.50
DDoS	Cloudflare (Comercial)	4.80	4.70	4.50	4.60	4.80	4.20
	Arbor Networks (Comercial)	4.70	4.60	4.00	4.20	3.00	4.50
WAF	Radware (Comercial)	4.60	4.50	4.00	4.10	2.80	4.60
	AWS WAF (Comercial)	4.50	4.30	4.30	4.50	3.80	4.10
	F5 WAF (Comercial)	4.30	4.00	3.80	4.00	2.90	4.30
	ModSecurity (Código abierto)	4.17	4.17	3.67	4.00	4.50	3.50
Herramientas de hacking ético	Kali Linux (Código abierto)	4.70	4.00	4.00	4.50	5.00	3.80
	Metasploit Pro (Comercial)	4.60	4.10	3.90	4.20	3.30	3.90
	Burp Suite (Comercial)	4.30	3.90	4.00	4.10	3.50	3.70
CTI	OpenCTI (Código abierto)	4.20	4.00	3.80	4.30	4.50	3.80
	MISP (Código abierto)	4.00	4.10	3.60	4.20	4.70	3.70
	SOCRadar (Comercial)	4.50	4.30	4.00	3.80	2.80	4.00
	Fuentes de CTI (FIRST, Shadowserver)	4.00	3.90	3.90	4.10	5.00	3.60

Los resultados de la encuesta mostraron una clara preferencia por las herramientas de código abierto en todos los ejes evaluados. Wazuh obtuvo las puntuaciones más altas en escalabilidad (4,5) y rentabilidad (4,83), seguido de cerca por ELK Stack y ModSecurity. En contraste, herramientas comerciales como Splunk y QRadar fueron valoradas por su capacidad técnica, pero penalizadas por su costo y complejidad de implementación.

En el área de plataformas y servicios de inteligencia de amenazas, OpenCTI y MISP fueron las plataformas mejor valoradas en términos de flexibilidad, interoperabilidad y sostenibilidad en entornos con recursos limitados. Los feeds públicos como los de FIRST, Shadowserver y Team Cymru obtuvieron las puntuaciones más altas en rentabilidad (5,0), destacándose como una base viable para CSIRT que buscan enriquecer sus análisis sin incurrir en gastos adicionales.

En cuanto a herramientas ofensivas y de entrenamiento, Kali Linux (4,7), Metasploit Pro (4,6) y Burp Suite (4,3) fueron reconocidas como esenciales para la validación de controles y ejercicios de concienciación. Cobalt Strike, por otro lado, mostró resultados mixtos debido a su sofisticación, alto costo y potencial de uso indebido en ausencia de políticas claras de gobernanza.

Finalmente, entre las soluciones de mitigación de DDoS, Cloudflare obtuvo las mejores puntuaciones en funcionalidad, escalabilidad y facilidad de uso, mientras que Arbor y Radware se destacaron por sus capacidades avanzadas de mitigación, aunque limitadas por su modelo de negocio. AWS WAF fue particularmente bien recibido por su integración nativa con servicios en la nube, mientras que F5 fue percibido como una solución robusta pero con altas dependencias técnicas.

4. Conclusiones

Las plataformas de código abierto ofrecen el mejor valor general para los CSIRT académicos, al combinar una sólida capacidad técnica con la flexibilidad presupuestaria que requieren los entornos de educación superior. Los datos de encuestas y entrevistas muestran una clara preferencia por soluciones que puedan desplegarse de forma incremental, ampliarse mediante complementos comunitarios y mantenerse sin compromisos costosos de licenciamiento.

SIEM

Wazuh es considerado de primer nivel debido a sus amplias funcionalidades, escalabilidad y bajo costo. Elastic Stack ocupa una posición cercana, reconocido por sus potentes capacidades analíticas y amplias integraciones. Splunk sigue siendo una opción viable para organizaciones que pueden asumir sus mayores gastos en licencias e infraestructura. Al implementar Wazuh o Elastic, se deben asignar recursos para que el personal personalice reglas y paneles. Los usuarios de Splunk deben anticipar gastos constantes por la ingestión de datos.

Solución	Plataforma
SIEM	Wazuh (Código abierto)
	Elastic (Comercial / Código abierto)
	Splunk (Comercial)

DDOS and WAF

Cloudflare ofrece un sólido equilibrio entre capacidad de mitigación y facilidad de uso frente a ataques DDoS volumétricos. Para necesidades de limpieza más complejas, aunque a un costo superior, Arbor (Netscout) es una excelente opción. En cuanto a la seguridad a nivel de aplicación, ModSecurity es una opción ligera y de código abierto, mientras que AWS WAF proporciona una integración perfecta para implementaciones en la nube. Un enfoque combinado de limpieza en las instalaciones o en la nube para ataques significativos, complementado con un WAF de código abierto en el borde de la red, puede abordar eficazmente los requerimientos típicos de un campus, manteniendo al mismo tiempo costos predecibles.

Solución	Plataforma
DDOS	Netscout (Comercial)
	Cloudflare (Comercial)

WAF	ModSecurity (Código abierto)
	AWS WAF (Comercial)

Herramientas de hacking ético

Los ejercicios de red team, la capacitación en concienciación y la verificación de controles siguen dependiendo en gran medida de Kali Linux, Metasploit o escáneres de red como NMAP y Greenbone. La persistente prevalencia de estas herramientas resalta el papel fundamental de la experiencia práctica en el desarrollo de las capacidades de los analistas.

Solución	Plataforma
Herramientas de hacking ético	Kali Linux (Código abierto)
	Metasploit Pro (Comercial)
	NMAP (Código abierto)
	Greenbone (Código abierto)

Servicios y plataformas de inteligencia de amenazas cibernéticas

Muchos flujos de trabajo de inteligencia de amenazas cibernéticas (CTI) en entornos académicos dependen de MISP y OpenCTI como componentes centrales, debido a su compatibilidad con los estándares STIX/TAXII y sus comunidades de usuarios activas. Se recomienda integrar fuentes de indicadores de alta calidad, como las de FIRST, Shadowserver y Team Cymru, para mejorar el contexto local y compensar posibles limitaciones en las capacidades de escaneo internas.

Solución	Plataforma
CTI servicios y plataformas	MISP (Código abierto)
	Shadowserver (feed)
	Team Cymru (feed)
	FIRST (MISP feed)

	OpenCTI (Código abierto)
--	--------------------------

Consideraciones para la implementación

- **Capacidades del personal:** Aunque las soluciones de código abierto reducen los costos de licenciamiento, requieren experiencia para su configuración y monitoreo continuo. Por ello, es fundamental invertir en la capacitación del personal.
- **Integración:** Se debe dar prioridad a soluciones que ofrezcan APIs abiertas para centralizar alertas y facilitar la automatización.
- **Niveles de presupuesto:** Las instituciones con presupuestos limitados pueden comenzar estableciendo una protección básica con Wazuh, ModSecurity y MISP. A medida que dispongan de más recursos, pueden fortalecer su postura de seguridad con herramientas como Elastic o servicios comerciales de limpieza.

Limitaciones y trabajos futuros

Los hallazgos se basan en conjuntos de herramientas en uso activo a mayo de 2025. Dada la rápida evolución de los planes de desarrollo de productos, modelos de licenciamiento (especialmente en el caso de Elastic) y del panorama de amenazas, se recomienda una reevaluación anual. Esto garantizará que la selección de plataformas se mantenga alineada con las necesidades cambiantes del sector académico.

5. Apéndice

Apéndice 1. Metodología - criterios de evaluación detallados

Funcionalidad: Evalúa el alcance y la profundidad de las capacidades técnicas: detección de amenazas, análisis de comportamiento, automatización, cumplimiento normativo e informes.

- 5: Motor de análisis avanzado, automatización, múltiples funciones nativas.
- 3: Funcionalidad básica, dependiente de complementos.
- 1: Solo una función, sin análisis de contexto ni correlación.

Integración: Mide la facilidad de conexión con otras herramientas (SIEM, WAF, registros, endpoints, APIs) y con los flujos de trabajo existentes.

- 5: APIs abiertas, múltiples conectores, complementos nativos, compatibilidad con entornos híbridos.
- 3: La integración es posible, pero requiere ajustes manuales.
- 1: Integración muy limitada o inexistente.

Usabilidad: Analiza la curva de aprendizaje, claridad de la interfaz, documentación, disponibilidad de capacitación y facilidad de implementación.

- 5: Interfaz intuitiva, buen soporte, capacitación accesible.
- 3: Uso intermedio, requiere conocimientos técnicos previos.
- 1: Muy compleja o sin soporte para usuarios no expertos.

Escalabilidad: Mide qué tan bien se adapta la solución a un entorno académico con eventos, usuarios o nodos en crecimiento.

- 5: Escalamiento horizontal/vertical sencillo, arquitecturas distribuidas.
- 3: Escalable con ajustes significativos.
- 1: Útil solo en entornos pequeños o controlados.

Costo: Considera los costos directos (licencias, soporte) e indirectos (infraestructura, personal), así como la disponibilidad de licencias educativas o de código abierto.

- 5: Gratuito o de muy bajo costo, con opciones comunitarias o académicas.
- 3: Costo moderado, accesible con financiamiento externo o proyectos.
- 1: Costo muy alto, inviable sin una inversión significativa.

Soporte y comunidad: Evalúa el acceso a soporte técnico, mantenimiento, actualizaciones, foros, documentación y la frecuencia de nuevas versiones.

- 5: Soporte 24/7, comunidad activa, documentación extensa.
- 3: Soporte limitado o solo comunitario, actualizaciones esporádicas.
- 1: Sin soporte claro, documentación desactualizada.

Apéndice 2. Preguntas de entrevista

Como parte de la segunda fase de la metodología, la consulta a las partes interesadas, se utilizaron las siguientes preguntas durante las **entrevistas**.

Rol

¿Cuál es tu rol en el CSIRT y tu nivel de participación en la selección o uso de soluciones de ciberseguridad?

- Adquisiciones
- Implementación técnica, uso operativo
- Toma de decisiones sobre políticas, etc.

Soluciones existentes

¿Qué soluciones de ciberseguridad están actualmente en uso? (por ejemplo, SIEM, WAF, mitigación de DDoS, plataformas de hacking ético, plataformas CTI, etc.)

- Lista de soluciones:
 - Nombre de la solución
 - Proveedor
 - Fecha de primer uso
 - Detalles de versión/lanzamiento
 - Nivel de satisfacción
- ¿Se utilizan múltiples soluciones simultáneamente para el mismo propósito?
 - Si es así, ¿por qué? (por ejemplo, diferentes casos de uso, interno vs. externo, redundancia)
- Tipo de solución:
 - ¿Comercial, de código abierto o híbrida?
- Proceso de selección:
 - ¿Cómo se eligieron estas soluciones?
 - ¿La decisión entre comercial y código abierto se tomó de antemano o fue influenciada por la disponibilidad en el mercado?
- Flexibilidad de adquisición:
 - ¿Pueden adquirir soluciones mediante acuerdos de compra conjunta con instituciones académicas, agencias gubernamentales u organizaciones afiliadas? En caso afirmativo, ¿esto les resulta beneficioso o restrictivo?
 - ¿Están obligados a seleccionar soluciones de un catálogo centralizado (organización matriz) o tienen total flexibilidad para elegir?

Efectividad

¿Qué tan efectivas han sido estas soluciones para mejorar la postura de ciberseguridad de tu CSIRT?

¿Puedes compartir incidentes específicos en los que estas herramientas jugaron un papel clave? No el incidente exacto, sino el tipo de incidente.

¿Colaboraste con el proveedor (o con los equipos del proyecto de código abierto) durante el incidente? Por ejemplo, ¿habilitaste funciones específicas que no estaban activadas inicialmente? ¿Extensiones/integraciones temporales para la herramienta?

- ¿Hay herramientas (desplegadas) que encontraste ineficaces o inadecuadas para tu entorno?
 - ¿Por qué?

Integración

¿Qué tan bien se integran estas soluciones con tu infraestructura y flujos de trabajo existentes?

- ¿Desafíos importantes en el despliegue o interoperabilidad?
- ¿Tuviste que desarrollar soluciones alternativas o herramientas adicionales para que funcionaran eficazmente?

Licencias

¿Cuál ha sido tu experiencia con los modelos de licenciamiento?

- ¿Usan principalmente licencias anuales, licencias perpetuas o soluciones de código abierto?
- ¿Has enfrentado restricciones presupuestarias para mantener o actualizar estas herramientas?

Demostración y evaluación

¿Realizaron una prueba de concepto (PoC), demostración o evaluación antes de adquirir o desplegar la solución (incluidas soluciones de código abierto en producción)?

- Para soluciones de código abierto:
 - ¿Qué tan colaborativos fueron los mantenedores durante la fase de PoC?
- Para soluciones tanto comerciales como de código abierto:
 - ¿Recibieron soporte en sitio para abordar los desafíos de integración?
 - ¿Cuáles fueron los factores clave que influyeron en la decisión final?

Soporte

¿Cómo evalúas el soporte del proveedor y el soporte de la comunidad para estas soluciones?

- Para herramientas de código abierto, ¿recibes soporte adecuado de la comunidad o de terceros?
- Para soluciones comerciales, ¿cómo calificarías la capacidad de respuesta y la efectividad del soporte del proveedor?

Escalabilidad

¿Qué tan escalables son las soluciones que usas?

- ¿Se adaptan bien a las necesidades del equipo a medida que evolucionan las amenazas y aumenta el volumen de datos?
- ¿Has tenido que reemplazar o actualizar herramientas debido a problemas de escalabilidad?

Intercambio

¿Puedes compartir información, alertas o reportes generados por estas herramientas con tu comunidad o con otros CSIRT?

- Por ejemplo, ¿proporcionas reportes periódicos sobre ataques DDoS o fuentes de inteligencia de amenazas?
- ¿Existen barreras técnicas o normativas para el intercambio de información?

Desafíos

¿Cuáles son los mayores desafíos al adoptar nuevas soluciones de ciberseguridad?

- ¿Restricciones legales, presupuestarias o técnicas que afecten la capacidad de implementar nuevas herramientas?
- ¿Cómo garantizan el cumplimiento con las regulaciones regionales?

Futuro

Si tuvieras la oportunidad de mejorar tu conjunto de herramientas, ¿qué capacidades o mejoras adicionales priorizarías?

- ¿Hay herramientas o funcionalidades específicas que faltan en el mercado actual?

Apéndice 3. Preguntas de encuesta

Como parte de la segunda fase de la metodología, la consulta con partes interesadas, se utilizó una encuesta para recopilar más resultados. Esta encuesta usó la metodología descrita anteriormente y pidió a los participantes que evaluaran las soluciones en funcionalidad, integración, facilidad de uso, escalabilidad, costo, soporte y comunidad.

- SIEM
 - Wazuh - Código abierto
 - Splunk - Comercial
 - QRadar - Comercial
 - Elastic - Código abierto
- DDoS
 - Cloudflare - Comercial / Gratuito
 - Arbor Networks (Netscout) - Comercial
 - Radware - Comercial
- WAF
 - ModSecurity - Código abierto
 - AWS WAF - Comercial (PaaS)
 - F5 WAF - Comercial
- Herramientas de hacking ético
 - Kali Linux - Código abierto
 - Metasploit Pro - Comercial
 - Burp Suite - Comercial / Free
 - Cobalt Strike - Comercial
- Plataformas y servicios de inteligencia de amenazas cibernéticas
 - ShadowServer Foundation - Con coste (requiere ser propietario de ASN)
 - FIRST - Gratuito (requiere membresía)
 - Team Cymru - Gratuito
 - Recorded Fusion - Comercial
 - MISP - Código abierto
 - Recorded Future - Comercial
 - Zerofox - Comercial
 - OpenCTI - Código abierto
 - SOCRadar - Comercial

Estudio de referencia sobre plataformas de ciberseguridad para CSIRTs académicos

Koen Van Impe, Carlos Leonardo

© EU CyberNet 2025

Las opiniones y puntos de vista expresados son exclusivamente del autor y no reflejan necesariamente los de la Unión Europea ni de EU CyberNet. Ni la Unión Europea ni EU CyberNet se responsabilizan de ellos.