Diseño de un Centro de Operaciones de Seguridad (SOC) basado en herramientas de Código Abierto

Resumen

Ante el creciente aumento de ciberataques en el sector educativo, la Universidad Autónoma de Ciudad Juárez (UACJ) emprendió un proyecto para diseñar un Centro de Operaciones de Seguridad (SOC) utilizando herramientas de código abierto. El objetivo principal es fortalecer la protección de los datos y servicios institucionales con una inversión mínima en licencias, aprovechando soluciones gratuitas y colaborativas. En este documento se detalla el desarrollo del proyecto: desde la identificación de objetivos y la justificación basada en estadísticas de ciber amenazas, hasta la selección e integración de plataformas tecnológicas abiertas (como Wazuh, Elastic Stack, Greenbone y MISP) que conforman el SOC propuesto. También se describen las actividades realizadas, los recursos materiales y humanos empleados, los aprendizajes obtenidos y los próximos pasos sugeridos. Como resultado, se presenta un diseño completo de un SOC adaptado a la realidad de la UACJ, demostrando la viabilidad técnica y estratégica de implementar seguridad avanzada mediante software libre y la importancia de la colaboración interuniversitaria en ciberseguridad.

Desarrollo del proyecto

Objetivos del proyecto

El propósito central del proyecto es diseñar un SOC para la UACJ que eleve significativamente su capacidad de monitoreo y respuesta ante incidentes de seguridad, con un enfoque de bajo costo sustentado en software de código abierto. Dado que las instituciones de educación superior manejan grandes volúmenes de datos sensibles y servicios críticos, un SOC permitirá detectar amenazas en tiempo real y reaccionar oportunamente para asegurar la continuidad de las actividades universitarias. Un objetivo clave es reducir la exposición de la UACJ a ciberataques en un contexto de crecientes amenazas cibernéticas. Asimismo, el diseño busca minimizar costos aprovechando herramientas libres, de modo que los recursos financieros se destinen a infraestructura y capacitación en lugar de licencias de software (ANUIES, 2023). Otro objetivo relevante es fomentar la colaboración con redes académicas de ciberseguridad, integrando a la UACJ en iniciativas como la Red Nacional de Educación e Investigación (RNEI) de CUDI y la Organización Europea para la Investigación Nuclear (CERN), para compartir inteligencia de amenazas y fortalecer la defensa colectiva (ANUIES, 2023; CUDI, 2023).

Soluciones tecnológicas implementadas

La solución propuesta se basa en un conjunto de herramientas de código abierto integradas para conformar el SOC de la UACJ. Estas plataformas se eligieron por su madurez, funcionalidad y costo cero en licencias, cubriendo todas las capacidades clave de seguridad: monitoreo, detección, análisis y respuesta. Las principales herramientas son:

- **Wazuh (XDR/SIEM):** plataforma de detección y respuesta extendida que recolecta logs de servidores y dispositivos, detecta intrusiones y vulnerabilidades, y ejecuta respuestas automáticas a incidentes críticos (Wazuh, 2025).
- **Elastic Stack (ELK):** suite que incluye Elasticsearch, Logstash y Kibana para indexar y visualizar eventos de seguridad en tiempo real. Actúa como SIEM al

correlacionar logs de múltiples fuentes y presentar alertas en dashboards (Elastic NV, 2025).

- **Greenbone/OpenVAS:** sistema de gestión de vulnerabilidades que escanea la infraestructura de TI en busca de debilidades conocidas (Greenbone Networks, 2025).
- **MISP:** plataforma de inteligencia de amenazas que permite compartir indicadores de compromiso (IPs maliciosas, hashes de malware, etc.) con otras organizaciones (MISP Project, 2025).

En la arquitectura integrada, los agentes de Wazuh envían datos al servidor central y a Elasticsearch; las alertas se visualizan en Kibana; los escáneres de Greenbone aportan hallazgos de vulnerabilidades; y MISP provee contexto externo para enriquecer el análisis.

Actividades llevadas a cabo

El proyecto se desarrolló en varias etapas. Primero, un análisis del panorama de amenazas confirmó que el sector educativo enfrentó un volumen de ataques muy alto en 2024 (Check Point Software Tech, 2024). En México, el volumen de intentos de intrusión también resultó muy alto ese año (Riquelme, 2025), evidenciando la urgencia de fortalecer las capacidades de seguridad en la UACJ. Seguidamente, en un diagnóstico institucional, se destacó la necesidad de proteger los servicios universitarios críticos cuyo compromiso podría paralizar las operaciones.

Tabla 1. Ataques cibernéticos por país, muestra. Fuente: Check point.

País	*Promedio de ataques por organización*
India	6874
México	3507
Estados Unidos	1667

Para respaldar esta urgencia ante las autoridades, se presentaron casos recientes: en 2024 un ataque filtró expedientes académicos y financieros en la Universidad de Chile, y en 2025 un ransomware cifró datos sensibles en la Universidad Latina (UNILA) (Bloka, 2025). En la etapa de selección tecnológica, tras evaluar diversas alternativas de software libre, se decidió emplear Wazuh, Elastic Stack, Greenbone y MISP como núcleo del SOC, definiendo los roles de cada herramienta y su integración. En paralelo, se incorporaron lineamientos de colaboración externa: conectar la plataforma MISP con el CSIRTde CUDI (CUDI, 2023) el CERN. Finalmente, se definió el diseño de la arquitectura y el plan de implementación. Se estableció una arquitectura distribuida: agentes Wazuh instalados en servidores clave envían registros a un servidor central para correlación e indexación en Elastic Stack. Se programaron escaneos periódicos de vulnerabilidades con Greenbone y la integración de MISP para el intercambio automatizado de indicadores de compromiso. Además, se elaboraron protocolos de respuesta para distintos incidentes. Todas estas definiciones quedaron plasmadas en el documento final del diseño del SOC, listo para su presentación a la alta dirección de la UACJ.

Recursos utilizados (materiales y personales)

Para la ejecución del proyecto y la futura operación del SOC se contemplaron diversos recursos:

- **Recursos tecnológicos**: se emplearon exclusivamente herramientas de software libre, principalmente Wazuh, Elastic Stack, Greenbone y MISP. Se aprovechó la infraestructura existente de la UACJ (servidores físicos/virtuales y redes de comunicaciones) para desplegar las plataformas del SOC y recolectar los datos de seguridad. Asimismo, se dispuso de estaciones de trabajo para los analistas, con las configuraciones necesarias para acceder a las consolas de monitoreo y administración.
- **Recursos humanos**: el proyecto involucró a personal del área de la Dirección General de Tecnologías de la Información (DGTI) de la UACJ, en particular al personal de la Jefatura de Función de Ciberseguridad creada en octubre del 2024. Durante la fase de diseño, solo una persona se encargó del análisis de amenazas, selección de herramientas y elaboración del plan. Para la operación continua del SOC, se estimó necesario conformar un equipo de al menos 3–5 analistas que cubran turnos de 7 am a 10 pm, bajo la supervisión de un jefe del SOC encargado de la coordinación y enlace con las autoridades universitarias. La capacitación del personal es un componente esencial: se planificó impartir entrenamiento específico en el uso de las herramientas del SOC y en los procedimientos de respuesta a incidentes, aprovechando los recursos de aprendizaje disponibles en las comunidades open source. Asimismo, se contó con el apoyo colaborativo de MetaRed y el material proporcionado para llevar a cabo la “Campaña de Concientización de Ciberseguridad”, lo que permitió intercambiar conocimientos y buenas prácticas con otras instituciones para enriquecer la propuesta.

Conclusiones

Principales aprendizajes

El proyecto dejó múltiples aprendizajes. En primer lugar, se corroboró la importancia de contar con un SOC en el entorno universitario actual: las amenazas son constantes y evolucionan rápidamente, por lo que la preparación proactiva es clave para evitar daños mayores (Riquelme, 2025). También se comprobó que es viable implementar seguridad de nivel institucional con dichas herramientas, dado que plataformas como Wazuh, ELK, Greenbone y MISP han alcanzado una madurez y funcionalidad comparables a alternativas comerciales (Greenbone Networks, 2025; Wazuh, 2025). Otro aprendizaje clave fue el valor de la colaboración: vincularse con redes como la RNEI y el CERN permitió a la UACJ tener visibilidad de amenazas emergentes que afectan a otras universidades, evidenciando que la ciberseguridad es un esfuerzo conjunto (CUDI, 2023). Finalmente, se constató que la concienciación institucional es fundamental. Presentar a las autoridades cifras concretas y casos cercanos resultó efectivo para obtener su apoyo, demostrando que invertir en ciberseguridad no es un gasto sino una necesidad estratégica para salvaguardar la misión académica.

Próximos pasos

Con el diseño del SOC completado, los siguientes pasos se enfocan en llevarlo a la práctica. Primero, es necesario gestionar la aprobación y financiamiento del proyecto ante la Rectoría de la UACJ, enfatizando los beneficios y el bajo costo de implementación gracias al uso de software libre. Después de obtener la aprobación, se iniciará la implementación técnica: desplegar los servidores para Wazuh y Elastic, instalar los agentes en los sistemas críticos y configurar cada herramienta. En paralelo, se debe capacitar al equipo de seguridad, asegurando que los analistas dominen las plataformas y los procedimientos de respuesta a incidentes. También se recomienda establecer acuerdos formales de colaboración con la RNEI/CUDI y el CERN, a fin de institucionalizar el intercambio de

alertas. Finalmente, se plantea una etapa de evaluación continua: una vez en marcha el SOC, medir periódicamente su desempeño (tiempos de detección, número de incidentes gestionados, reducción de vulnerabilidades, etc.) para identificar mejoras y mostrar el valor del SOC, facilitando su crecimiento futuro.

Resultados alcanzados

El resultado principal fue un diseño integral de SOC adaptado a la UACJ, que identifica una combinación óptima de tecnologías abiertas capaz de brindar capacidades comparables a las de un SOC corporativo. Asimismo, el proyecto entregó lineamientos estratégicos y operativos: se definieron objetivos claros, un plan de despliegue, protocolos de respuesta y recomendaciones para integrar al personal y a la organización en la operación del SOC. Otro resultado importante fue la sensibilización de la comunidad universitaria sobre la relevancia de la ciberseguridad. La difusión del material facilitado por metared y el de elaboración propia generó conciencia y urgencia, facilitando la adopción de las medidas propuestas. Finalmente, el proyecto estableció vínculos con iniciativas externas (como la colaboración con el CERN y CUDI), posicionando a la UACJ dentro de un ecosistema de cooperación que potenciará la eficacia de su SOC una vez implementado. En conjunto, estos resultados representan un avance significativo hacia el fortalecimiento de la defensa cibernética de la UACJ.

Referencias

1. ANUIES. (2023, 28 de septiembre). Convocatoria: “Alianza México CiberSeguro”. Recuperado en mayo de 2025, de http://www.anuies.mx/noticias/convocatoria-aalianza-mxico-ciberseguroa
2. Bloka. (2025, 28 de abril). Ciberataques a instituciones educativas en América Latina: casos, impacto y tendencias. LinkedIn. Recuperado en mayo de 2025, de https://es.linkedin.com/pulse/ciberataques-instituciones-educativas-en-am%C3%A9rica-latina-casos-impacto-cus5f
3. Check Point Software Tech. (2024, 13 de agosto). Check Point Research: “Every Day is a School Day for Cyber Criminals…Education Sector as Top Target in 2024” [Blog]. Recuperado en mayo de 2025, de https://blog.checkpoint.com/research/check-point-research-warns-every-day-is-a-school-day-for-cybercriminals-with-the-education-sector-as-the-top-target-in-2024
4. CUDI. (2023, 6 de diciembre). CUDI y el CERN firman Acuerdo de Intercambio de Inteligencia sobre Amenazas. Recuperado en mayo de 2025, de https://cudi.edu.mx/noticias/acuerdo-cern-cudi
5. Elastic NV. (s.f.). Elastic Stack (ELK) – Elasticsearch, Kibana, Beats, Logstash [Sitio oficial]. Recuperado en mayo de 2025, de https://www.elastic.co/elastic-stack
6. Greenbone Networks. (s.f.). Protect Your IT Infrastructure: Open-Source Vulnerability Management [Sitio oficial]. Recuperado en mayo de 2025, de https://www.greenbone.net/
7. MISP Project. (s.f.). MISP – Open Source Threat Intelligence Platform [Sitio oficial]. Recuperado en mayo de 2025, de https://www.misp-project.org/
8. Riquelme, R. (2025, 29 de abril). México recibió 324,000 millones de intentos de ciberataques en 2024: Fortinet. El Economista. Recuperado en mayo de 2025, de https://www.eleconomista.com.mx/tecnologia/mexico-recibio-324-000-millones-intentos-ciberataques-2024-fortinet-20250429-756919.html
9. Wazuh. (s.f.). The Open Source Security Platform – Unified XDR and SIEM [Sitio oficial]. Recuperado en mayo de 2025, de https://wazuh.com/