Solucion	Ventajas	Inconvenientes	Version	Fecha de version
Metron	Capacidad de gestionar y analizar alertas	No automatizacion	0.7.1-release	8 mayo 2019
	Posibilidad de anadir nuevos parsers	Recursos especificos y software especifico para poder usarlo		
	Almacenamiento de datos enriquecidos	Intefaz de usuario no proporciona autenticacion		
	Deteccion de anomailas basado en algoritmos de aprendizaje de maquina			
MozDef	Se puede desplegar en la nube	Interfaz de usurio poco intuitiva	v3.1.2	4 octubre 2019
	Automatizacion de eventos con python	Puesta a punto mas complicada		
	Facilita la tarea del equipo analista			
	Hace de intermediario entre las aplicaciones de coleccion de datos y logStash para poder alterar la informacion con scripts de Python y analisis usando aprendizaje automatico			
	Muy modular			
AlienVault OSSIM	Descubrimiento de dispositivos	No escala bien	N/A	10 abril 2017
	Analisis de vulnerabilidades	Poco soporte para almacenemiento de eventos		
	correlation SIEM "Open Threat Exchange"	Ejecucion en un unico servidor		
	Deteccion de intrusion	No tiene integracion con UEBA		
	Monitorizacion de comportamiento	Monitorizacion de aplicaciones y base de datos pobre		
	Herramienta de colaboracion Open Threat Exchange	Base de datos de analisis poco resolutiva		
		No da soporte a herramientas DAM, CASB, DAP, and DLP		
Wazhu	Disponible para la nube	Disponible en la nube si pagas	v.4.0.3	30 noviembre 2020
	Disponible en gran variedad de dispositivos	Carace herramientas de gestion de incidentes e intrusiones (Tickets)		
	Despliegue moderno, con Chef, Ansible, docker o Puppet			
	Interfaz de usuario clara y moderna			
Security Onion	Sistema operativo auto-contenido	Debe estar en constante evolucion, a diferencia de otros SIEM, no proporciona opcion a analisis automatico	16.04.7.2	14 diciembre 2020
	Altamente configurable	Requisitos hardware bastante elevados		
	Altamente escalable	Coste de correr el servicio elevado, al menos al inicio, cuando el trafico no es muy grande		
Empow	Automatizacion forma parte del producto desde el primer dia	Un unico ecosistema - El usuario no tiene eleccion a la hora de decidir que base de datos usar, o que harramienta de analisis de red usar	N/A	N/A
	Integracion con MITRE ATT&CK	Poca personalizacion. Si algo no te gusta, no lo puedes cambiar		
	Tecnologia basada en Inteligencia Artificial			
	Agrupa varios eventos en un solo ataque, basandose en IA			
IBM Q-Radar	Dashboard muy potente	No es customizable	7.4	10/2020
	Proporciona al analista mucho control sin la necesidad de que el analista tenga mucha experiencia con seguridad	La configuracion del sistema inicial es muy costosa, ya que se tiene que anadir a mano todas las propiedades de los sistemas sobre los que esta actuando QRadar		
	Incorpora IBM Watson, una tecnologia de analisis de datos en la nube	Obliga a la empresa a adentrarse en el ecosistema de IBM para poder usar todas las caracteristicas del SIEM		
Lacework	SIEM para entornos Cloud	No tan maduro como otros SIEM comerciales, como IBM Q-Radar	v3.3.5	11/2020
	Uso de tecnologias de aprendizaje automatico	Requiere analistas mas experimentados para su uso eficaz		
	Enfoque a anomalias, ventaja, porque es adaptable, no basado en reglas, pero necesita datos iniciales (Desventaja)	Requiere profesionales con conocimiento de arquitectura de red para entender el comportamiento o motivo de la amenaza		
	Uso de estandares reconocidos en el mundo de la ciberseguridad (CIS Benchmark)	Requiere expertos en ciberseguridad para gestionar la infraestructura		
	Proporciona el estado por cada hora del entorno cloud de la red	Requiere un uso mucho mas activo que otros SIEM comerciales, ya que Lacework proporcina hechos, que luego el analista debe conectar, creando una hipotesis y realizando una investigacion.		
	Modular, en el sentido en el que puede intergrarse con otros SIEM mas populares o conocidos como Splunk			
LogRythmn	Proporciona una interfaz grafica madura, con capacidad de seguir eventos e incidentes e investigarlos.	Analista debe tener una base fuertre de ciberseguridad, ya que los comandos, aunque no ejecutados directamente desde las maquinas infectadas, o desde una linea de comandos, si que se tienen que ejecutar manualmente en algunos casos	v7.6.0	N/A
	Proporciona la capadicad de trabajar conjuntamente frente a un unico incidente, de forma que un equipo puede ver en tiempo real las pruebas nuevas encontradas sobre el incidente	No es tan modular como otras alternativas		
	Proporciona la capacidad de actuar frente a incidentes detectados directmante desde la consola	Los requisitos de utilizacion del SIEM son mas elevados que los de algunas anternativas		
	Es el SIEM mas maduro existent en este analisis con capacidades Cloud			
Splunk	Visibilidad de todas las maquinas en la red	No tiene una gestion de incidentes tan madura como otras alternativas, como LogRythm	v8.1.0.1	10/2020
	Eficiencia y contexto a la hora de la captura de registros	Gestion de incidentes individual, no grupal		
	Flexibilidad, ergo adaptabilidad a los cambios de la red	Analistas deben ser profesionales de la ciberseguridad		
	Analisis de comportamiento de anomalias	Los pasos a seguir en la gestion del incidente no caben en la platforma, a diferencia de los "Playbooks" de LogRythm		
	SIEM Cloud			
	Relaciona multiples eventos en un unico incidente			
	Representacion de la informacion muy madura			