bastet®

Centraliced Cyber Vulnerability Manager

Tecnología, personas y procesos alineados para centralizar la responsabilidad compartida de la ciberseguridad.

Bastet® es una herramienta para la gestión de vulnerabilidades basada en la automatización y centralización de todos los procesos que intervienen en su ciclo de vida.

- **Operador de vulnerabilidades de punto único,** agregador de fuentes (Nesus, Qualys, Checkmarx...).
- **Refactorización de riesgos** en base a criterios corporativos.
- **Automatización de tareas** y generación de outputs orquestados**.**
- Mejorar la **visibilidad y accionabilidad** de los equipos responsables.

Beneficios

- **Para las operaciones:** Reduce los costes de explotación/ Evita los conflictos de versiones de las revisiones/ Reduce la tasa de error/ Registro de seguimiento/ SSO incorporado.
- **Para la gestión:** Sistema centralizado/ Múltiples proveedores-origen/ Optimización de recursos/ Control de la información/ Portal seguro.
- **Para los equipos: PO/PM:** Previsión en vivo/ Requerimientos de seguridad/ Estado de la solución. **DESARROLLO:** Prueba de seguridad/ Parche de asistencia/ Seguimiento. **ALTA DIRECCIÓN:** Métricas en vivo/ Control de la demanda/ Reducción del ruido.
- **Analista de seguridad**: Enfoque de seguridad/ Herramienta de diagnóstico/ Programación y tareas/ Optimización del tiempo.

Developed by wisesecurity GLOBAL

hello@wsg127.com | +34 910 700 549 | wsg127.com

bastet®

Centraliced Cyber Vulnerability Manager

Funcionalidades

Estructura de datos:

- Generacion de assets de tipos configurables, relacionados con endpoints para el traking de vulnerabilidades y sus responsables.
- Permite trackear las revisiones de seguridad que generan vulnerabilidades.
- Gestión del ciclo de vida y priorización de las vulnerabilidades, así como traking del SLA sobre las correciones.

Autorización:

- Segmentación de visibilidades y permisos de manera multinivel.

Ingestión de datos:

- Integración con todas las fuentes relevantes de vulnerabilidades y activos.

Procesamiento de datos:

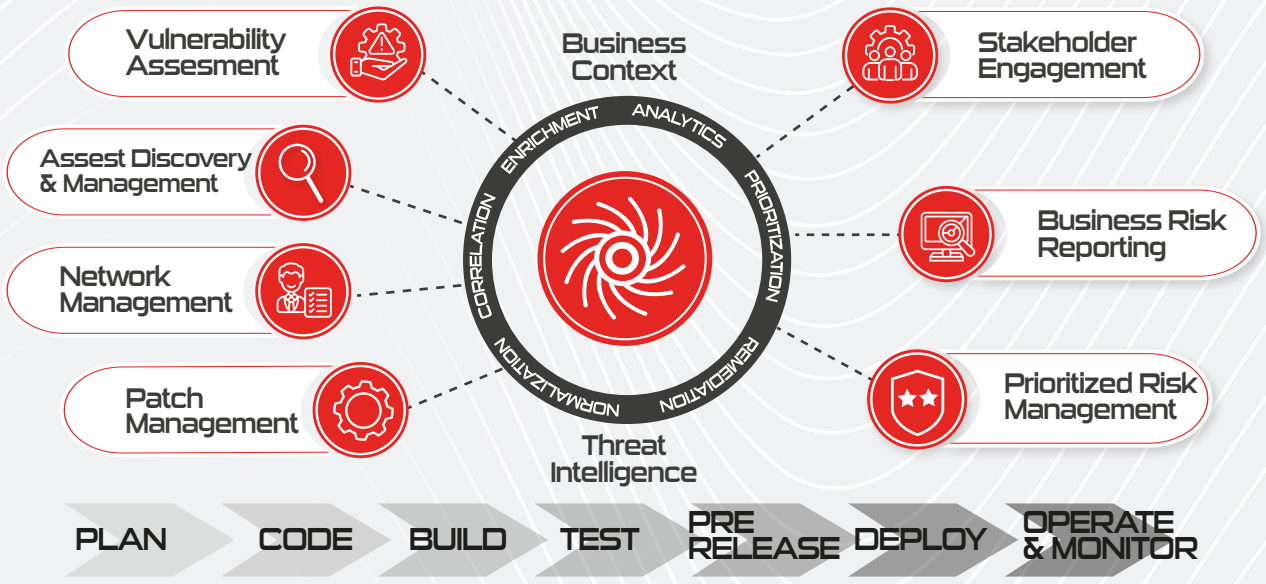
- Categorización de las vulnerabilidades en base a parámetros configurables tomando como base el scoring de las herramientas y generando un "custom risk" el cual se adapta a la tipología de red y la criticidad de los assets dentro de una organización.

Visualización:

- Visualización de datos a través de tablas y gráficos, de forma general y segmentada.

Reporting:

- Envío de reporting automático a los responsables de los productos. Posibilidad de envíos manuales de reporte sobre vulnerabilidades concretas para su gestión inmediata. Extracción de csv. Posibilidad de consumir la información vía API.



Solicita una demo

hello@wsg127.com | +34 910 700 549 | wsg127.com