bastet®

Centraliced Cyber Vulnerability Manager

Bringing together technology, people, and processes to centralize shared responsibility for cybersecurity.

Bastet® is a vulnerability management tool based on the automation and centralization of all the processes involved in the life cycle of a vulnerability.

- **Vulnerability single point operator,** source aggregator (Nesus, Qualys, Checkmarx...).
- **Risk refactoring** based on corporate criteria.
- **Task automation** and generation of orchestrated outputs.
- Improve **visibility and actionability** to the responsible teams.

Benefits

- **For operations:** Reduces operating costs/ Avoids conflicts of versions of revisions/ Reduction of the error rate/ Monitoring record/ SSO incorporated.
- **For management:** Centralised management/ Multiple supplier-origin/ Optimisation of resources./ Information control/ Secure portal.
- **For equipment:** **PO/PM:** Live forecast/ Security requirements/ Resolution status. **DEVELOPER:** Security test/ Assistance patch /Monitoring. **SENIOR MANAGEMENT:** Live metrics/ Demand control/ Noise reduction. **SEC ANALYST:** Security focus/ Diagnostic tool/ Programming and tasks/ Time optimisation.
- **Security analist**: Security Approach/ Diagnostic Tool/ Scheduling and Tasks/ Time Optimization.

Developed by wisesecurity GLOBAL

bastet®

Centraliced Cyber Vulnerability Manager

Features

Data Structure:

- Generation of assets of configurable types, related to endpoints for the tracking of vulnerabilities and their responsible.
- Allows tracking of security patches that generate vulnerabilities.
- Lifecycle management and prioritization of vulnerabilities, as well as SLA tracking on remediation.

Authorization:

- Segmentation of visibilities and permissions in a multilevel way.

Data ingestion:

- Integration with all relevant sources of vulnerabilities and assets.

Data processing:

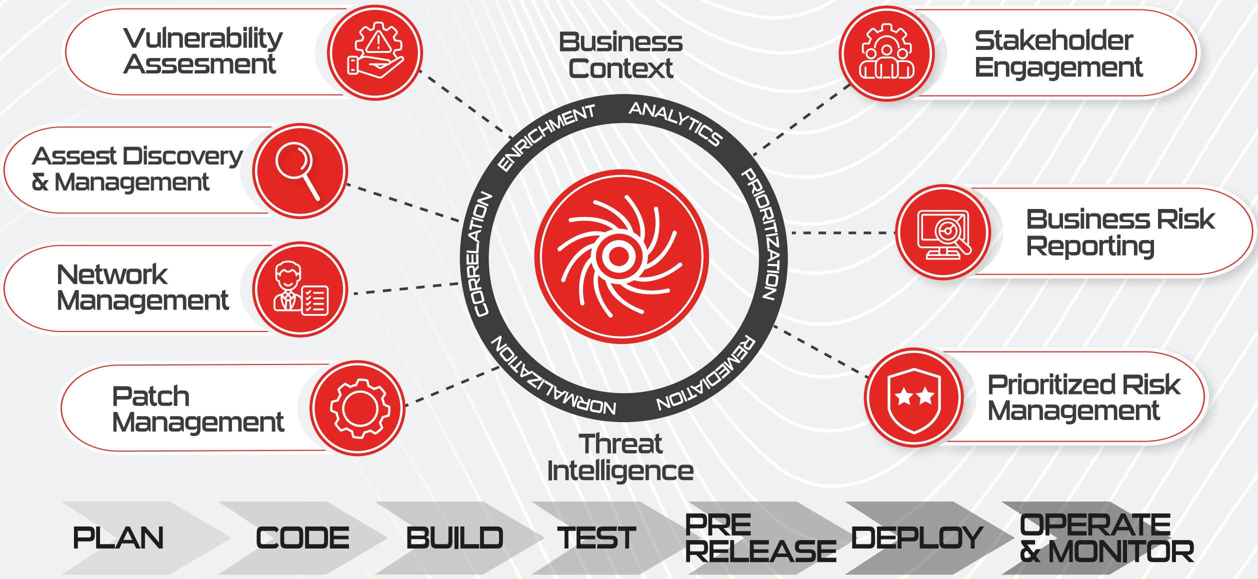
- Categorization of vulnerabilities based on configurable parameters taking as a basis the scoring of the tools and generating a "custom risk" which is adapted to the type of network and the criticality of the assets within an organization.

Visualization:

- Data visualization through tables and some graphs, generally and segmented.

Reporting:

- Sending of automatic reporting to product managers. Possibility of manual sending of reports about specific vulnerabilities for immediate management. Csv extraction. Possibility of consuming the information via API.



Request a demo

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