

Product Introduction

WIKI - Reconnaissance Aerial Vehicle

WIKI-RAV

It is our ultimate goal

that eliminates the blind spots of information security

around the world by sharing Korea's experiences and know-how

WiKi Security Corporation

Information Security Solution Provider

Table of Contents

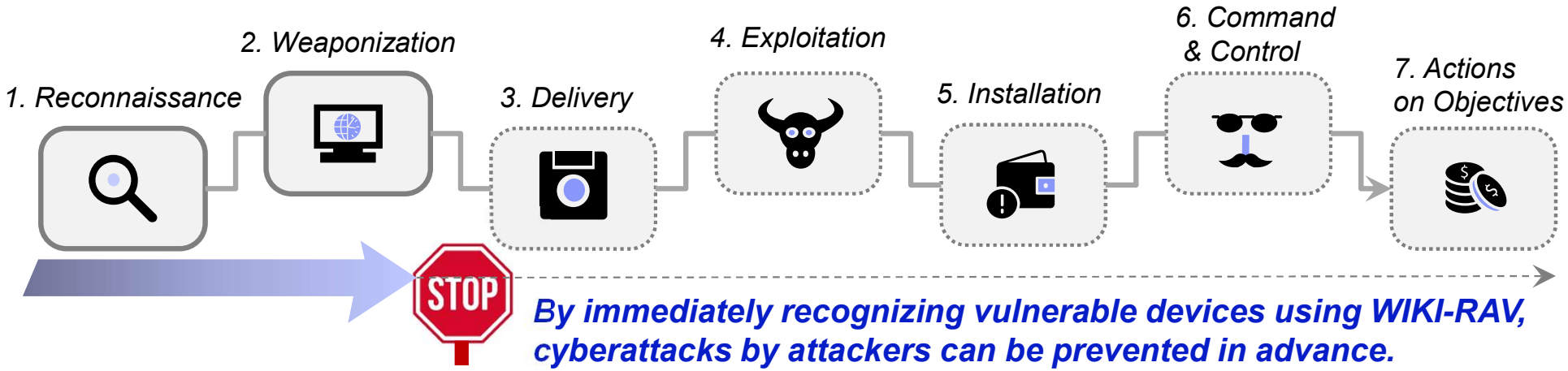
- ***What can you use this solution for?***
- ***What does the name of the solution mean?***
- ***Who needs this solution?***
- ***What are the differentiators of this solution?***
- ***Annex - Major Screenshots***
- ***Annex - Product Models***



What can I use this solution for?

❖ **Considering the Cyber Kill Chain, this solution can proactively prevent IP devices in your Large-Scale network from cyber attacks.**

- The Cyber Kill Chain (CKC) consisting of 7 steps is useful for establishing a systematic defense strategy by allowing the defender to understand the attacker's order of operations.
- By using this WIKI-RAV solution, it helps to identify and search IP devices exposed to vulnerabilities in advance, which is useful for preventing cyber attacks in step 1 (Reconnaissance) and step 2 (Weaponization) of the CKC.
- In particular, a CSIRT or a SOC, who manages numerous IP devices in the Large-Scale network, is effective in identifying and monitoring IP devices exposed to known vulnerabilities.

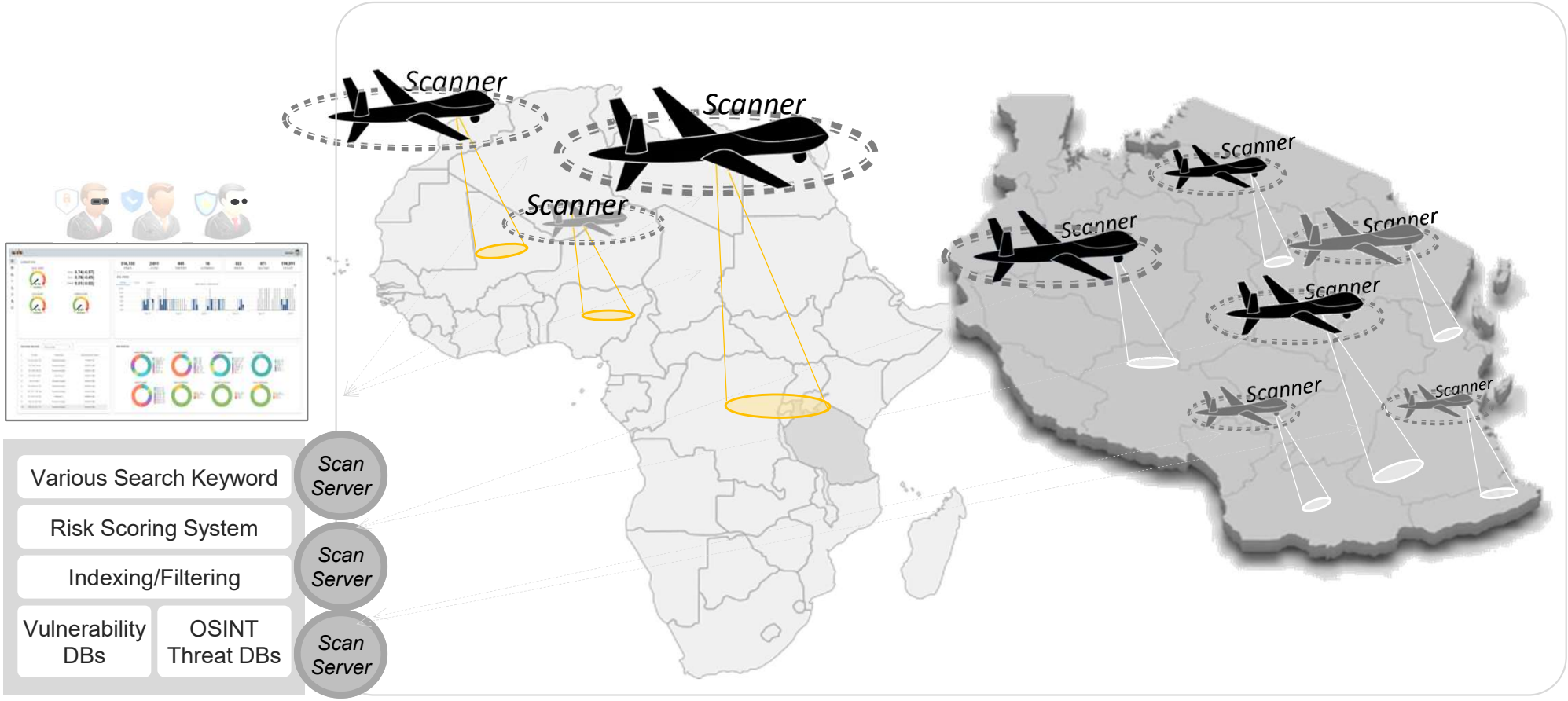


Copyright © 2022 WiKi Security Corporation All rights reserved

What does the name of the solution mean?

❖ WIKI-RAV(Reconnaissance Aerial Vehicles)

This solution collects status information and vulnerabilities of IP devices by 24X7 continuous scanning like an unmanned reconnaissance aircraft for large-scale networks such as cities, countries, states, and continents, and searches, analyzes, and monitors them.
Therefore, It is essential for CSIRT, SOC, ISP/IXP, and global companies.



Copyright © 2022 WiKi Security Corporation All rights reserved

Who needs this solution?

❖ **If your job is one of the following, then this solution is necessary for you.**

A. Are in charge of the National CSIRT task, which is responsible for national cyber safety from external cyber-attacks.

B. Are in charge of cybersecurity work in an ISP or IXP business environment that manages a large-scale IP network.

C. Are a cybersecurity manager of an Autonomous System that provides services by being assigned numerous IPs.

D. Are a cybersecurity officer in charge of the cybersecurity of the globally distributed large-scale network.

Cybersecurity Staff



National CSIRT

Cybersecurity Manager



Internet ISP, IXP

Cybersecurity Manager



Autonomous System

Cybersecurity Officer



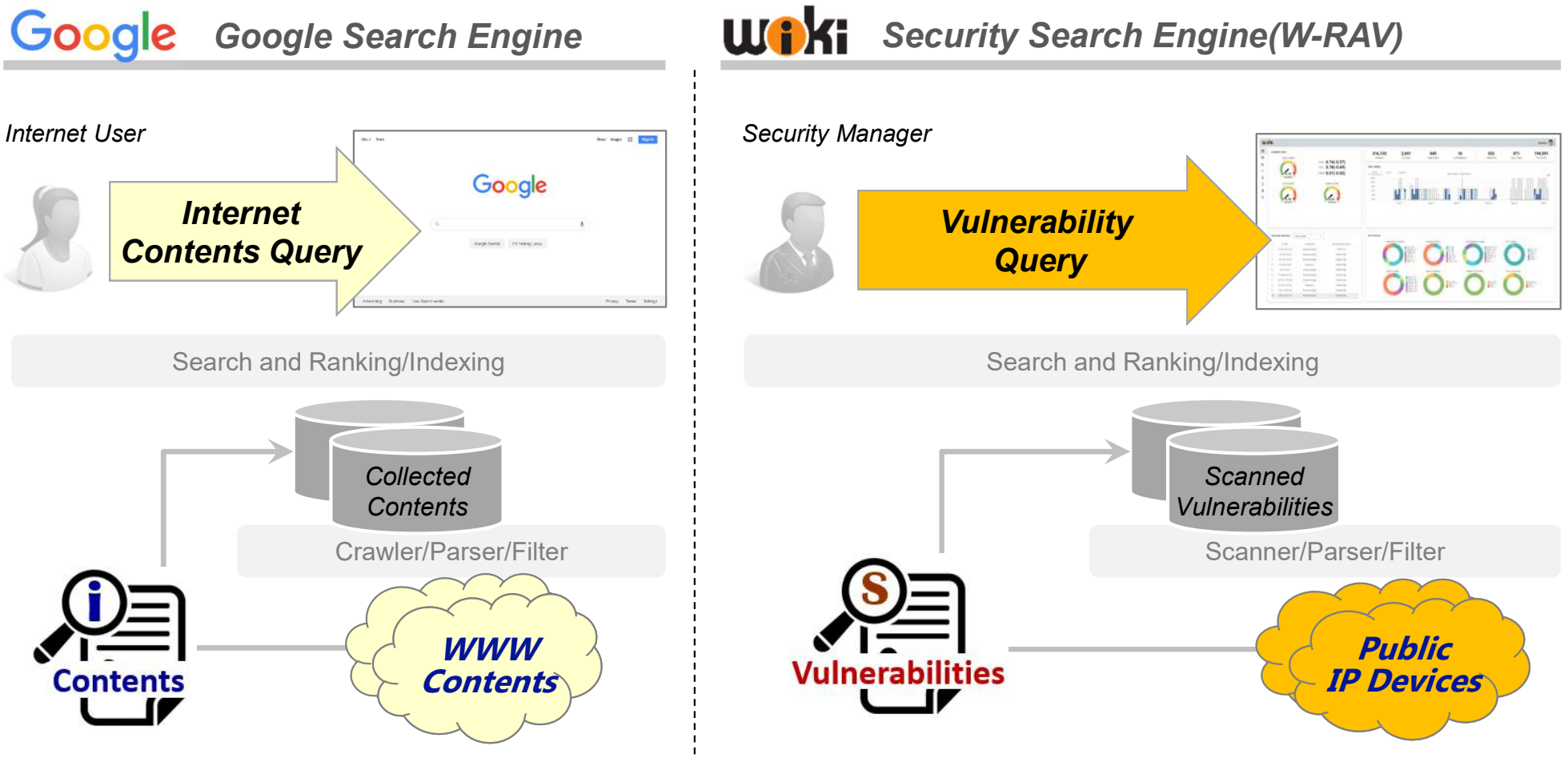
SOC Center

Copyright © 2022 WiKi Security Corporation All rights reserved

What are the differentiators of this solution?

❖ **Just as the Google is a search engine that searches contents on the Internet,**

This is a search solution that you can search and analysis on the general status and security vulnerabilities of all IP devices on the large-scale network you manage.

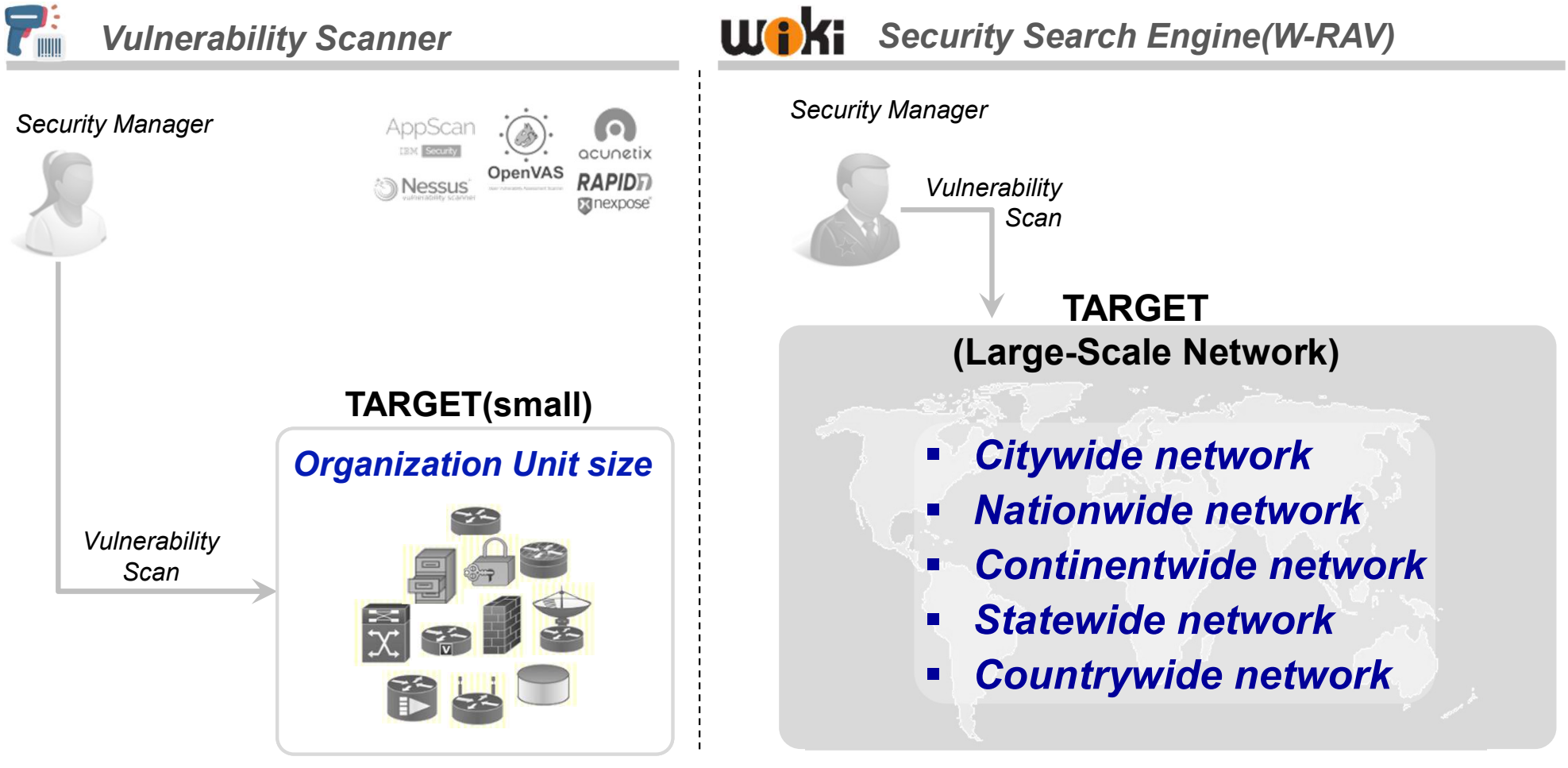


Copyright © 2022 WiKi Security Corporation All rights reserved

What are the differentiators of this solution?

❖ **Existing vulnerability scanner products target small scale,**

but this solution scans all IP device status and security vulnerabilities targeting Large-scale networks IP devices such as city, state, country, and continent.

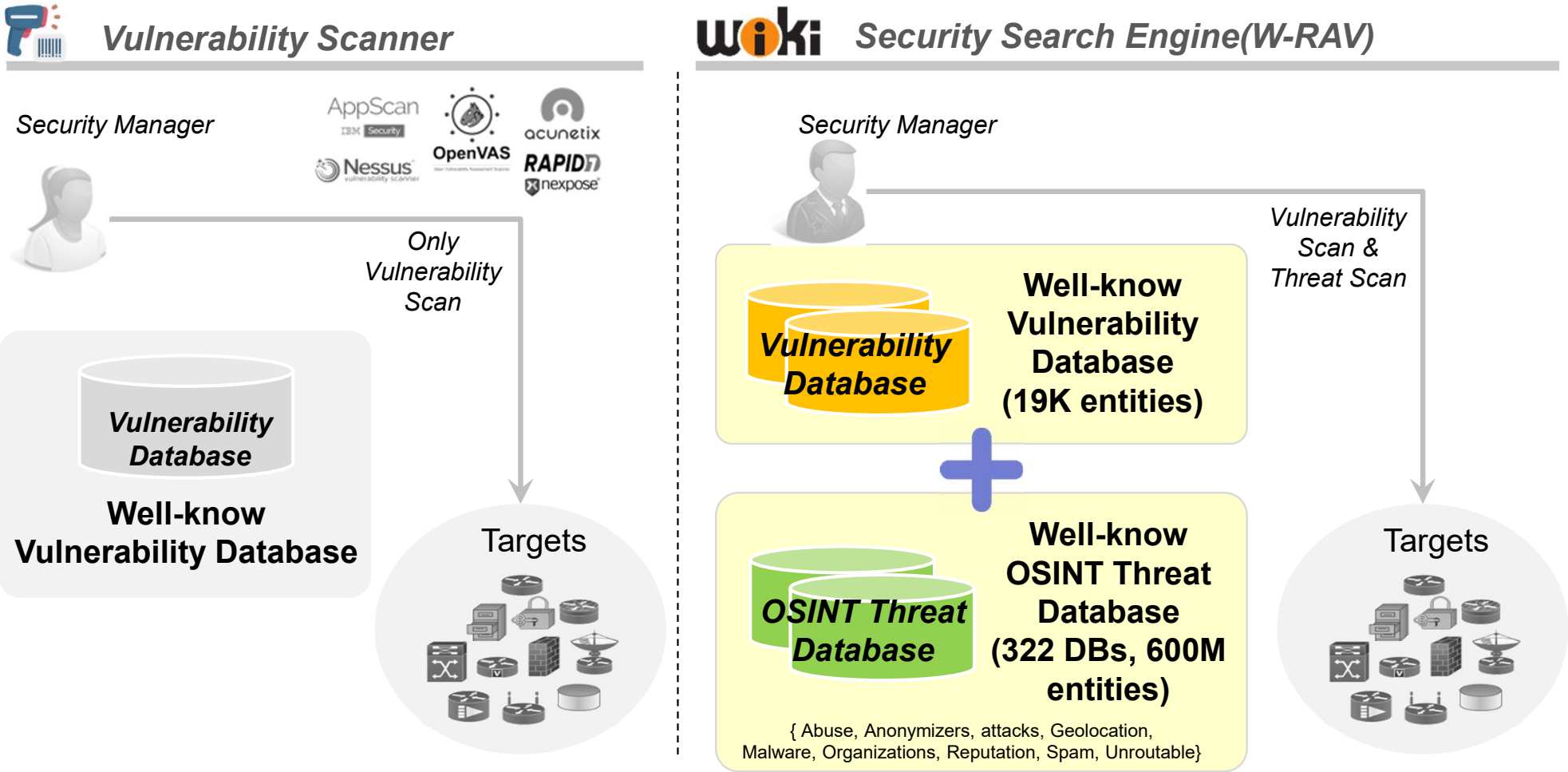


Copyright © 2022 WiKi Security Corporation All rights reserved

What are the differentiators of this solution?

❖ **Existing vulnerability scanning products use only the security vulnerability DB,**

Moreover, this solution updates and applies not only well-known vulnerability DBs such as CVE, but also 320 OSINT Threat DBs (600M entities) to the scan every day.



Copyright © 2022 WiKi Security Corporation All rights reserved

What are the differentiators of this solution?

❖ **The existing solutions have only cloud products and provides only the search function,**

However, this solution provides not only Cloud but also On-Premise products, so you can keep sensitive information by your side and manage it. Also, as the Risk Scoring System based on mathematical technology, it provides differentiated functions such as the overall risk monitoring.

Security Search Engine

SHODAN Censys Binary Edge

Provides only cloud-type products
Security vulnerabilities of all IP devices you manage are exposed to everyone

Provides only individual IP device search
Impossible to monitor the overall risk situation

No importance distinction between IP devices
Difficulty in selective intensive management of critical systems(CIIP* System)

Security Search Engine(W-RAV)

Cloud type and On-Premise (Self-hosting) type are provided according to customer's request
For government organizations such as National CSIRT, the On-Premise model is recommended

Application of the Risk Scoring System as well as Search function
Supports policy and decision-making related to vulnerability through the Dashboard showing comprehensive risk status and trend information

Provides separate identification and monitoring functions only for IP devices with high importance

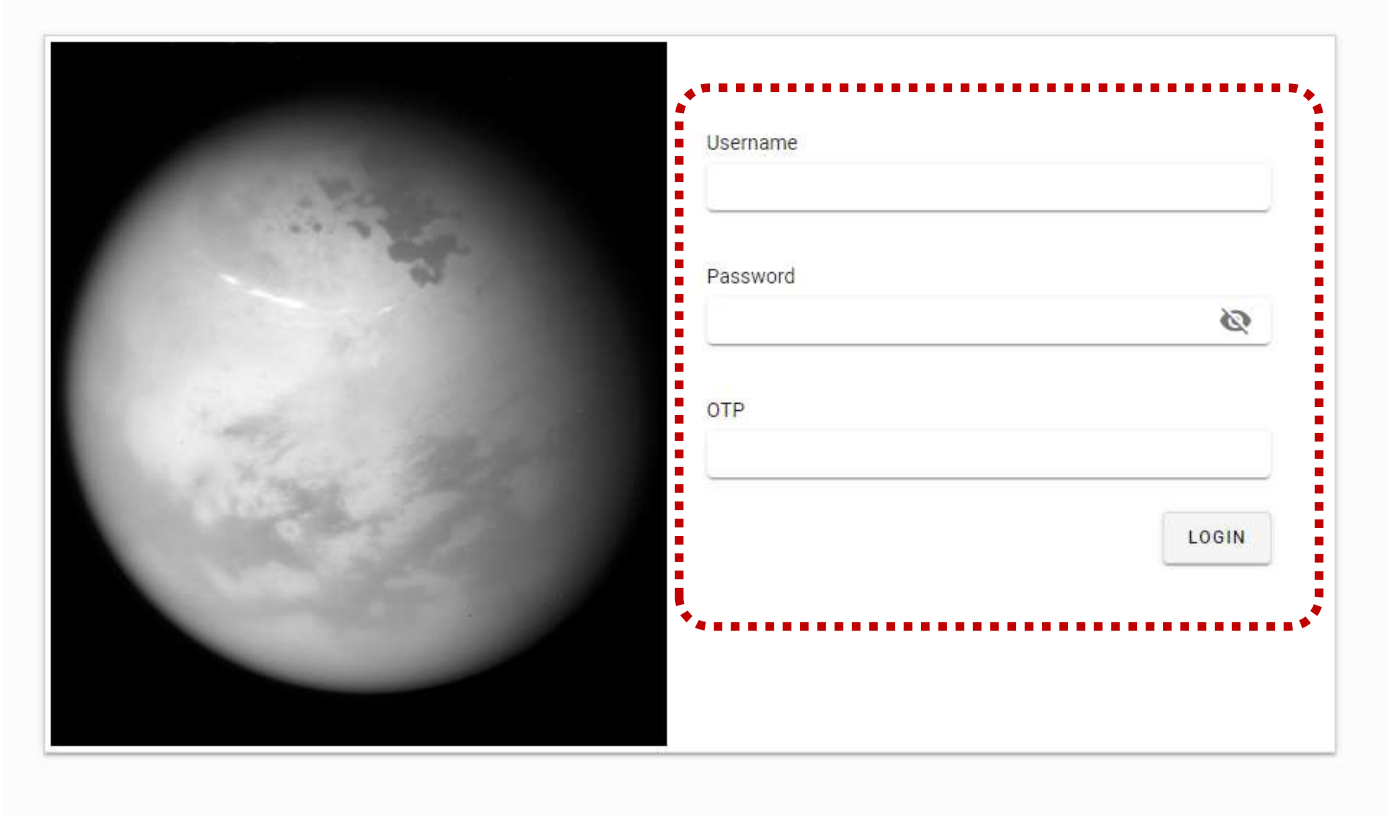
* CIIP: Critical Information Infrastructures Protection System

Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Major Screenshots

Login and Signup

- Since this solution handles sensitive information, only users registered by the system administrator according to the user registration procedure can access it.
- To strengthen the authentication of this solution, OTP (One Time Password) is used along with Username and Password.

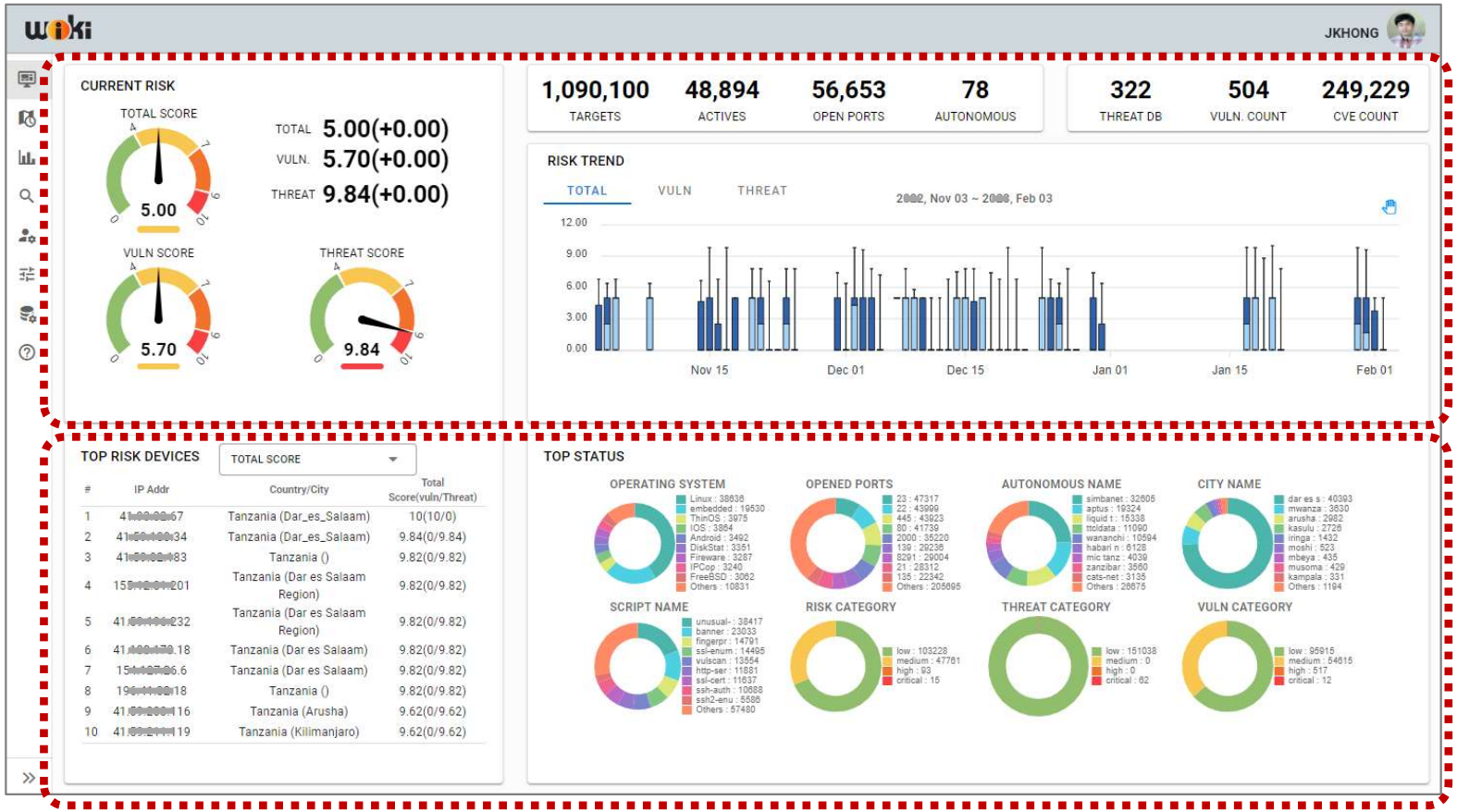


Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Major Screenshots

Menu: Status

- This menu summarizes and provides important information that the user needs to know.
- Through this menu, the user can see at a glance the current security risk level, the trend of risk from a time series perspective, the list of the Top 10 Devices in risk level, and the top statistical information.

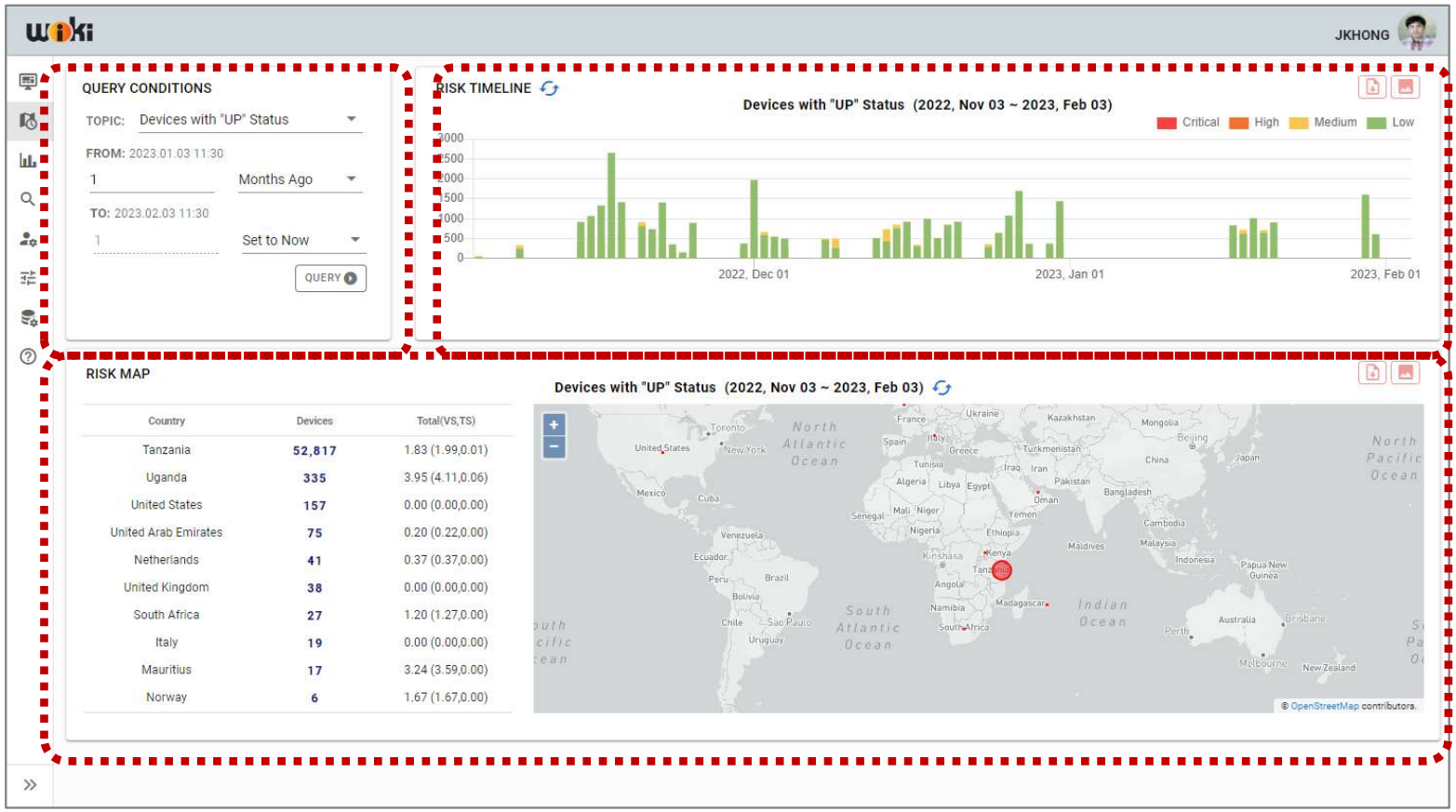


Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Major Screenshots

Menu: Timeline

- This menu provides the states that the user must observe carefully from both temporal and geographical perspectives.
- Through this menu, the user can search the results in a variety of ways by utilizing the given condition search, both temporally and geographically.



Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Major Screenshots

Menu: Search

- This menu provides the functionality of searching for detailed information about IP devices using keywords.
- The user can search for information such as the AS name, the geographical location, and detailed vulnerability scan results, threat scan results, etc. of individual IP devices using the over 60 diverse search keywords provided.

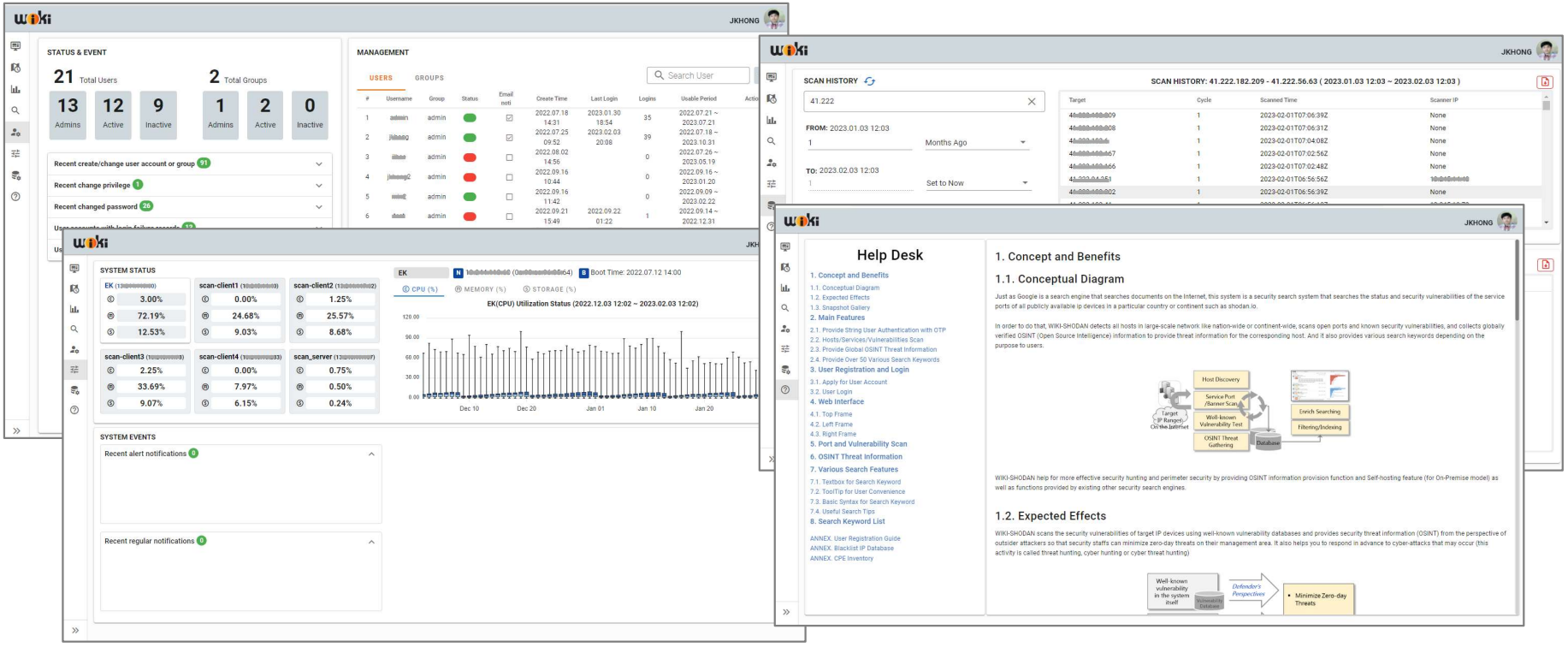


Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Major Screenshots

Menu: User&Group, System, Configuration, Help

- These menus provide the functionality for system administrators to manage user accounts and server states.
- Administrators can create/modify/delete user accounts through these menus and manage the health check and backup status of servers that configure the service.
- The Help menu provides system explanations, search keywords, CPEs, etc. necessary for both users and administrators.



Copyright © 2022 WiKi Security Corporation All rights reserved

Annex - Product Models

Depending on the characteristics of your organization and the size of the network you manage, the recommended model is below.

Organization	*Recommend*	*Standard Spec.*	*Network Size*
Union, Continent Organization	WIKI-RAV-OP-L1 (On-Premise Model)	▪ Web Svr: 2(2) ▪ Storage Svr: 5(5) ▪ Scan Server: 5(5) ▪ Scan Client: 20 X 6	> 100M IP Address
National CSIRT	WIKI-RAV-OP-M1 (On-Premise Model)	▪ Web Svr: 2(2) ▪ Storage Svr: 3(3) ▪ Scan Server: 3(3) ▪ Scan Client: 10 X 2	> 300K IP Address
CSIRT, SOC	WIKI-RAV-OP-S1 (On-Premise Model)	▪ Web Svr: 1(1) ▪ Storage Svr: 2(2) ▪ Scan Server: 2(2) ▪ Scan Client: 5 X 2	> 100K IP Address
Global Company	WIKI-RAV-OP-T1 (On-Premise Model)	▪ Web Svr: 1(1) ▪ Storage Svr: 3(3) ▪ Scan Server: 3(3) ▪ Scan Client: 5 X 2	< 10 C Class networks
	WIKI-RAV-OP-C1 (Cloud Model)	▪ Cloud Network	> 10 C Class networks

Copyright © 2022 WiKi Security Corporation All rights reserved

End of Document



CONTACT POINT

#1910, Ace Gasan Tower, 121, Digital-ro, Geumcheon-gu, Seoul, Republic of Korea
TEL : +82-2-322-4688 | Fax : +82-2-322-4646 | E-mail : info@wikisecurity.net | http://rura.wikisecurity.net