

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

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



Who needs this solution?

❖ 당신의 업무가 다음 중 하나에 해당한다면 이 시스템은 당신에게 절대적으로 필요한 시스템이다.

A. 외부 사이버 공격으로부터 국가 사이버 안전을 담당하는 국가 CSIRT 업무를 담당한다.

B. 대규모 IP 네트워크를 관리하는 ISP 또는 IXP 비즈니스 환경에서 보안 업무를 담당한다.

C. 다수의 IP를 할당 받아 서비스를 제공하는 Autonomous System의 보안관리자이다.

D. 전 세계적으로 분산된 대규모 네트워크의 보안을 담당하는 SOC의 보안 담당자이다.

Cybersecurity Staff

A 

National CSIRT

Cybersecurity Manager

B 

Internet ISP, IXP

Cybersecurity Manager

C 

Autonomous System

Cybersecurity Officer

D 

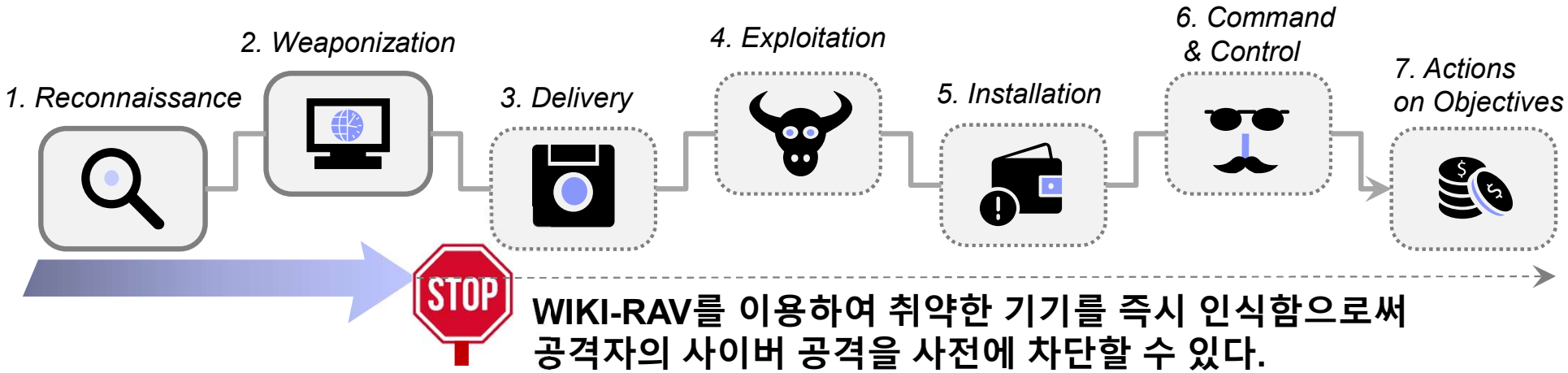
SOC Center

Copyright © 2022 WiKi Security Corporation All rights reserved

What can I use this solution for?

WIKI-RAV시스템을 이용하여 광범위한 Network Range의 보안 취약점 악용을 사전에 예방 할 수 있다.

- **7개 Step으로 구성된 Cyber Kill Chain(CKC)은 방어자가 공격자의 작업순서를 이해함으로써 체계적인 방어전략을 수립하는데 유용하게 사용된다.**
- **WiKi-RAV 솔루션을 이용하여, 취약점에 노출된 IP devices를 사전식별 및 검색할 수 있도록 도움으로써 그 CKC의 step1(Reconnaissance)와 step2(Weaponization)에서 사이버 공격을 사전방어하는 용도로 유용하다.**
- **특히, Large-Scale network의 수많은 IP device를 관리하는 CSIRT 또는 SOC는 이 솔루션을 통해 알려진 취약점에 노출된 IP Device를 식별하고 모니터링하는데 효과적이다.**



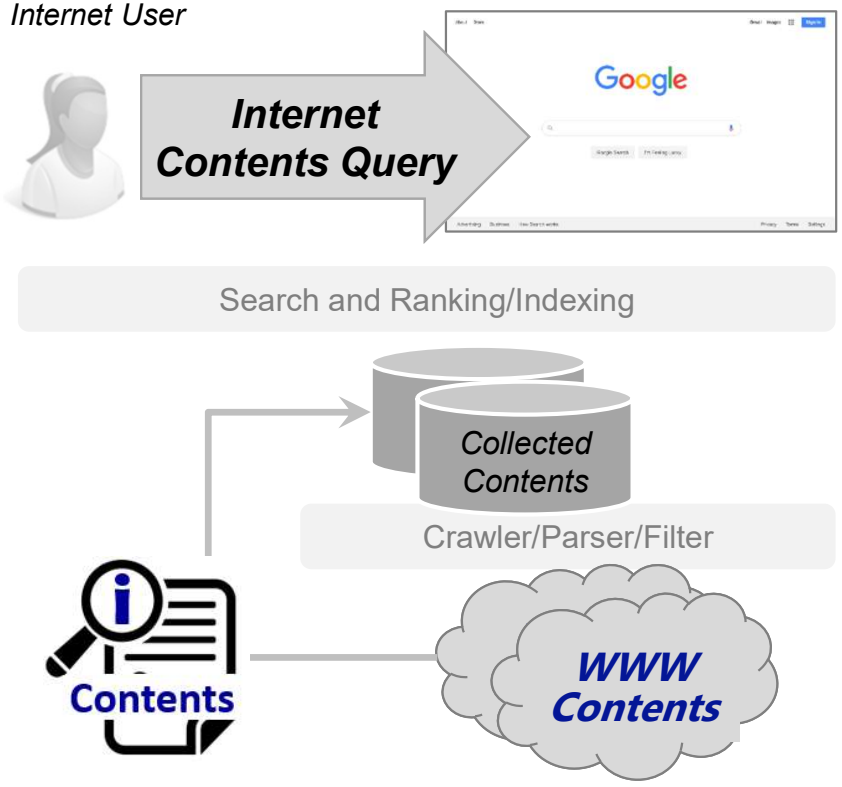
Copyright © 2022 WiKi Security Corporation All rights reserved

IT IS A SYSTEM THAT SEARCHES IP STATUS AND VULNERABILITIES

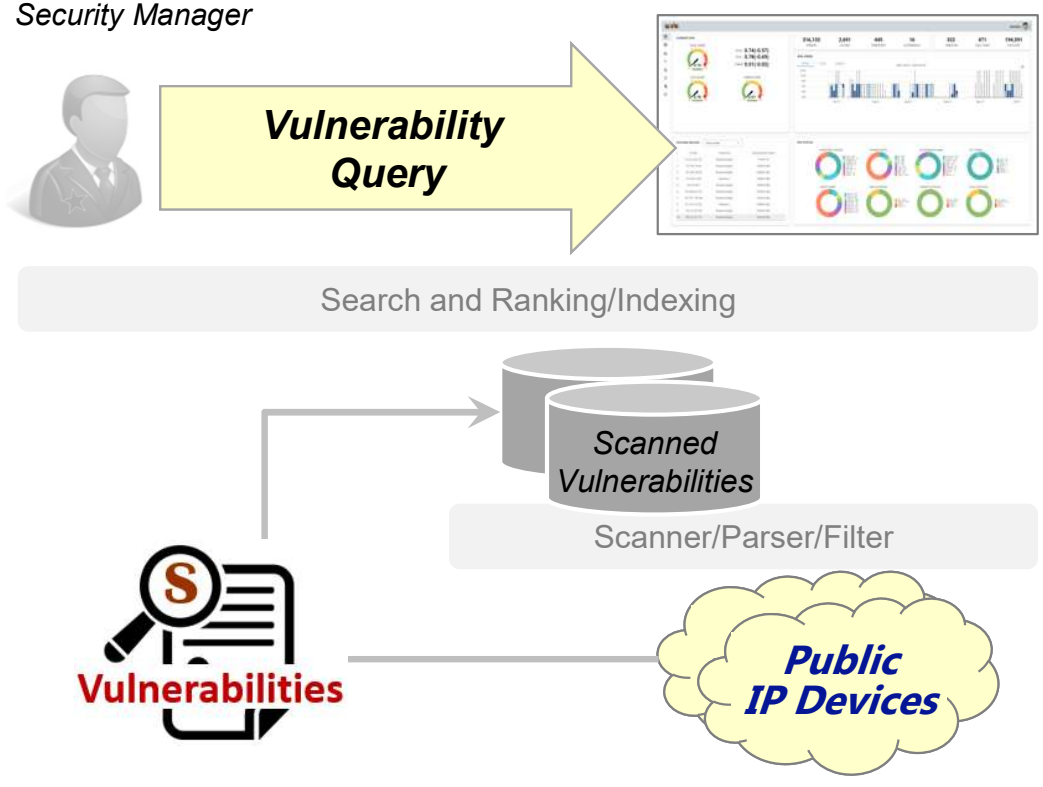
Google 검색이 인터넷의 콘텐츠를 검색할 수 있는 것처럼,

이 시스템은 당신이 관리하는 광범위한 네트워크에 있는 모든 IP 장치의 상태 및 보안 취약점을 검색한다.

Google Search Engine



Security Search Engine(W-RAV)



Copyright © 2022 WiKi Security Corporation All rights reserved

IT IS A SCANNER THAT LARGE-SCALE NETWORKS

기존 취약점 스캐너제품들은 작은 규모를 대상으로 하지만,

이 시스템은 도시단위, 주 단위, 국가단위, 대륙단위와 같은 대규모 네트워크의 IP device를 대상으로 모든 IP 장치의 상태 및 보안 취약점을 검색한다.

Vulnerability Scanner

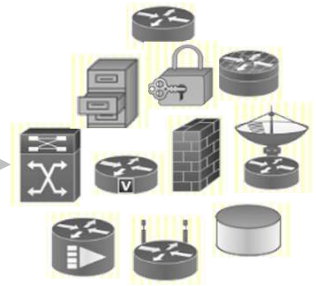
Security Manager

AppScan Security · Nessus vulnerability scanner · OpenVAS · acunetix · RAPID7 nexpose

Vulnerability Scan

TARGET(small)

Organization Unit size



Security Search Engine(W-RAV)

Security Manager

Vulnerability Scan

TARGET
(Large-Scale Network)

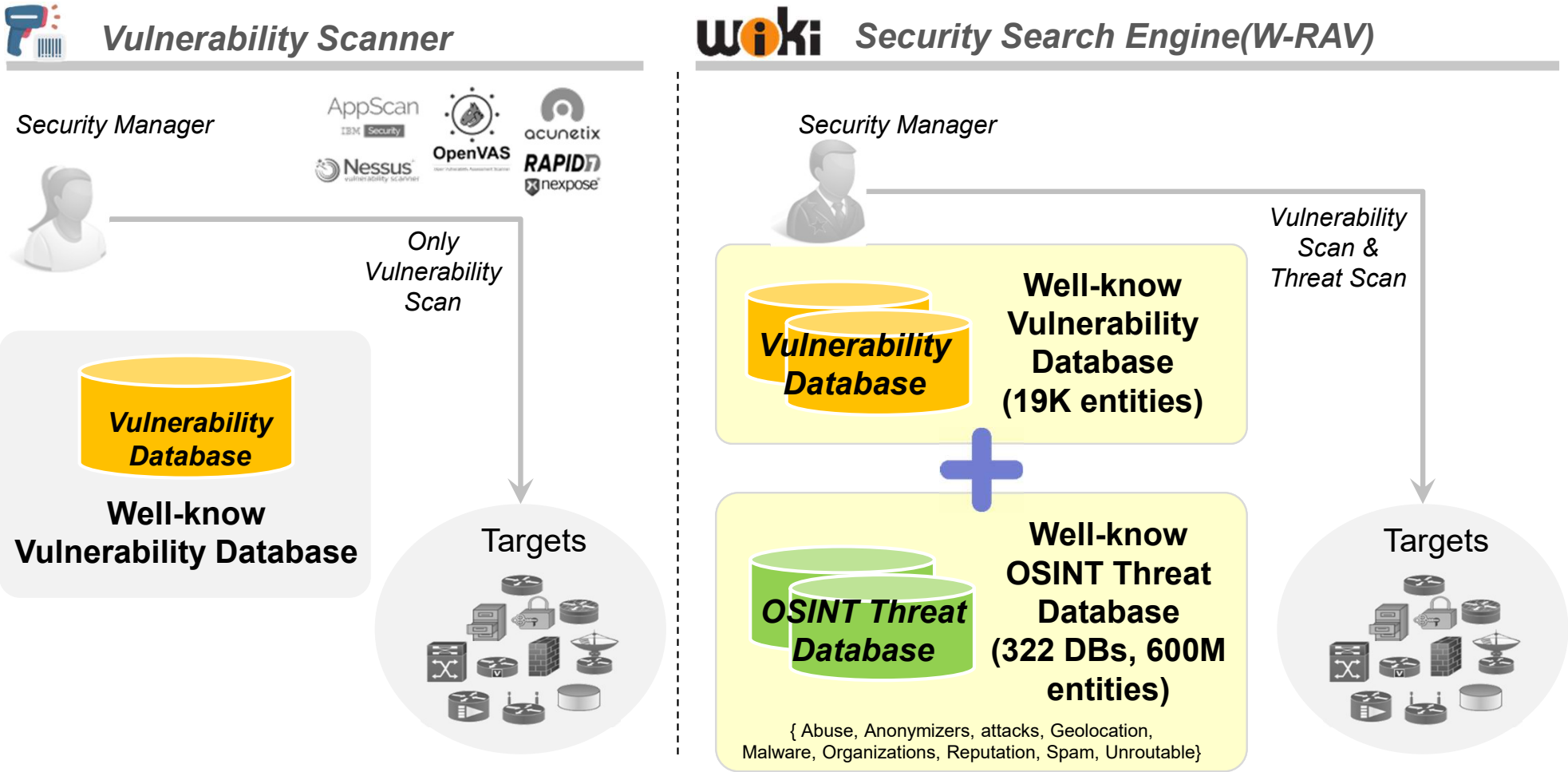
- ***Citywide network***
- ***Nationwide network***
- ***Continentwide network***
- ***Statewide network***
- ***Countrywide network***

Copyright © 2022 WiKi Security Corporation All rights reserved

IT SCANS NOT ONLY VULNERABILITY BUT ALSO THE OSINT THREAT

기존 취약점 스캔제품은 보안취약점 DB만 사용하지만,

이 시스템은 CVE와 같이 잘 알려진 취약점 DB뿐만 아니라 320여개 OSINT Threat DB(600M entities)를 매일 업데이트하여 스캔에 적용합니다.



Copyright © 2022 WiKi Security Corporation All rights reserved

IT IS SIGNIFICANTLY DIFFERENT FROM EXISTING PRODUCTS

기존 Security Search Engine은 Cloud 제품만 있고, Search기능만 제공하지만,

이 시스템은 Cloud뿐만 아니라 On-Premise제품도 제공하여 민감한 정보를 당신 옆에 두고 관리할 수 있으며, 수학적 기법 바탕의 Risk Scoring System으로 전체적 Risk 모니터링 기능 등 차별화된 기능들을 제공한다.

Security Search Engine

SHODAN Censys Binary Edge

Cloud 형태의 Subscription 판매 방식만 제공함
모든 대상 IP device에 대한 보안 취약점이 인터넷의 모든 사람에게 노출됨

개별 IP device에 대한 검색 기능만을 제공
관리하는 IP device 전체 위험상황에 대한 관리와 의사결정 지원이 불가능함

대상 IP device들에 대한 중요도 구별이 없음
주요정보통신기반시설과 같이 중요 모니터링 시스템에 대한 집중관리가 어려움

Security Search Engine(W-RAV)

고객사의 요구에 따라 Cloud 형태와 On-Premise (Self-hosting) 형태 제공
National CSIRT 등 정부조직의 경우 On-Premise를 선호함

검색기능 뿐만 아니라, 수학적 기법 기반의 Risk Scoring System 적용
Dashboard를 통해 종합적 위험상태와 추이 판단이 가능

중요도가 높은 IP device(예: CIIP*)의 식별 및 모니터링 기능으로 집중관리 가능
중요 시스템에 대한 위험도 모니터링 및 추이 관리 가능

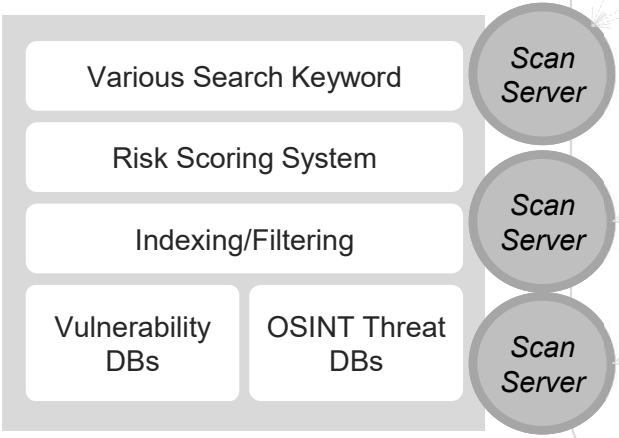
* CIIP: Critical Information Infrastructures Protection System

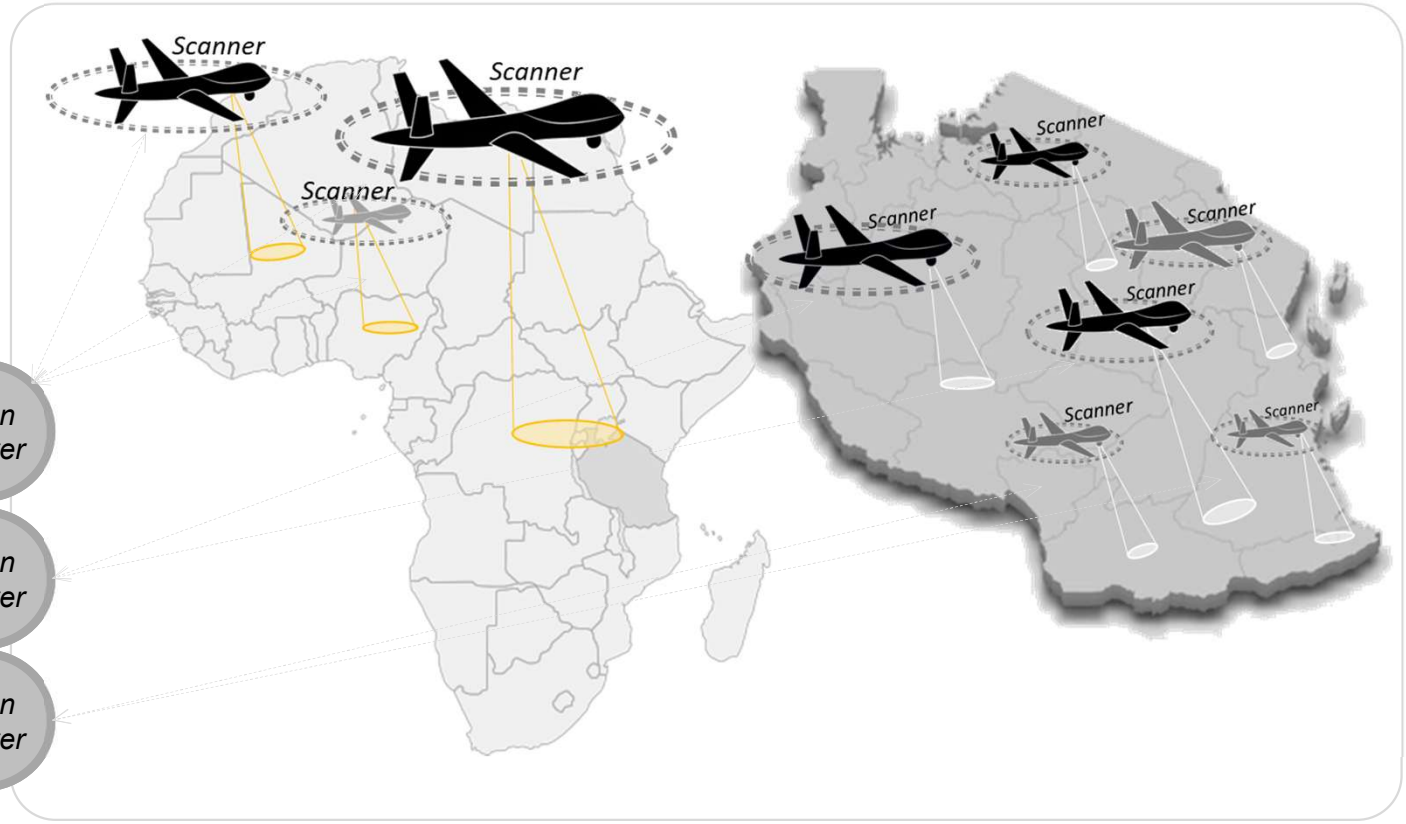
Copyright © 2022 WiKi Security Corporation All rights reserved

THE NAME IS WIKI-RAV(RECONNAISSANCE AERIAL VEHICLES)

이 시스템은 도시,국가,주,대륙 등과 같은 Large-scale Network를 대상으로 무인정찰기와 같은 여러 Scanner들이 24X7 상시 스캔하여 IP Device들의 상태정보 및 취약성을 수집하고 이를 검색, 분석, 모니터링 할 수 있는 시스템으로써, National CSIRT, SOC, ISP/IXP, 글로벌 컴퍼니에서 필요한 제품이다.



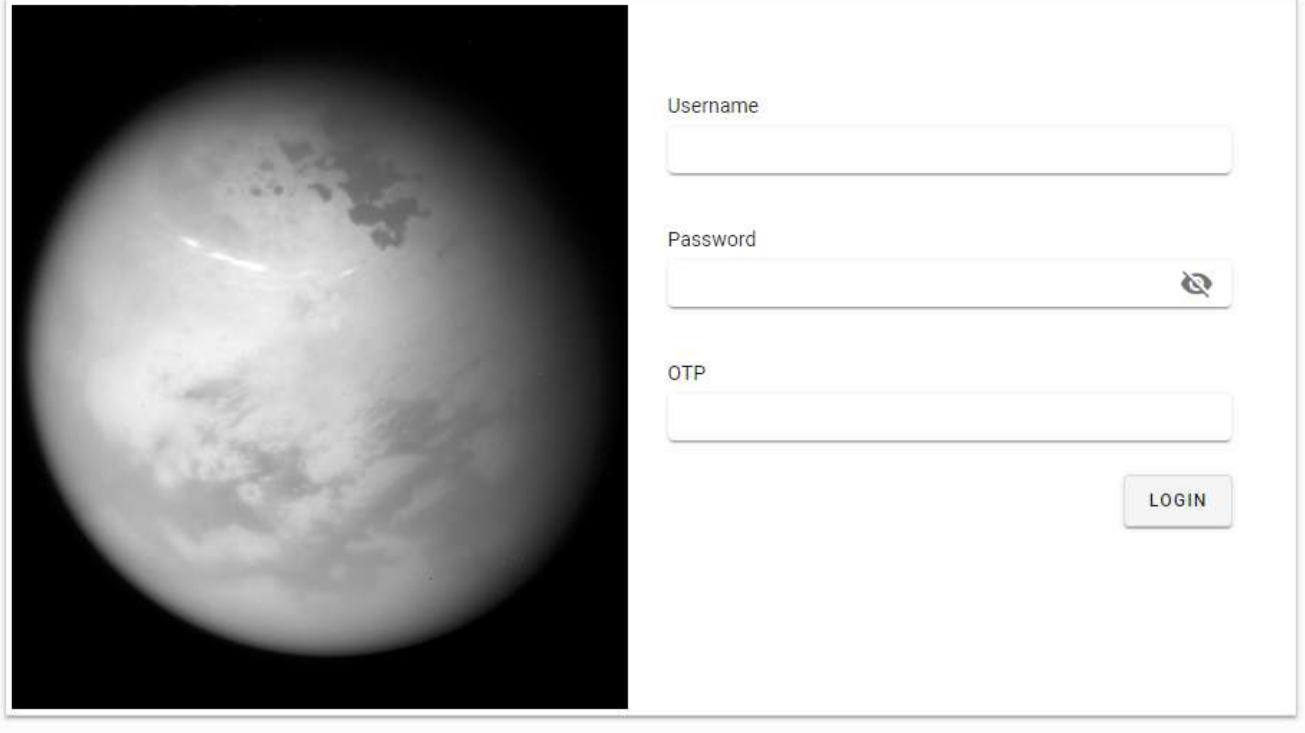




Copyright © 2022 WiKi Security Corporation All rights reserved

Login and Signup

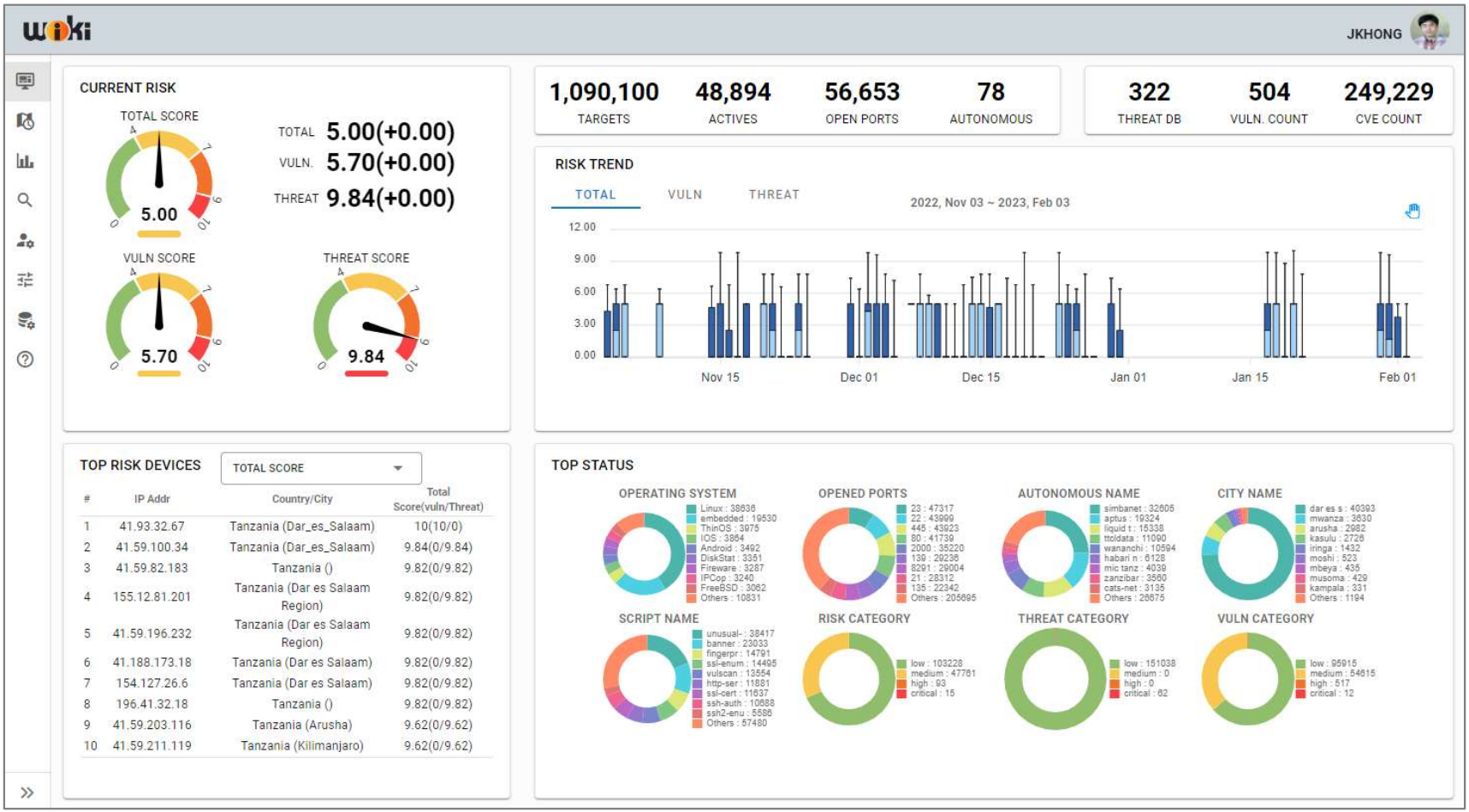
- 이 시스템은 민감한 정보를 취급하므로 사용자 등록절차에 따라 시스템관리자가 등록한 사용자만 접근이 가능하다.
- 이 시스템의 사용자 인증은 Username, Password와 더불어 OTP를 사용한다.



Copyright © 2022 WiKi Security Corporation All rights reserved

Menu: Status

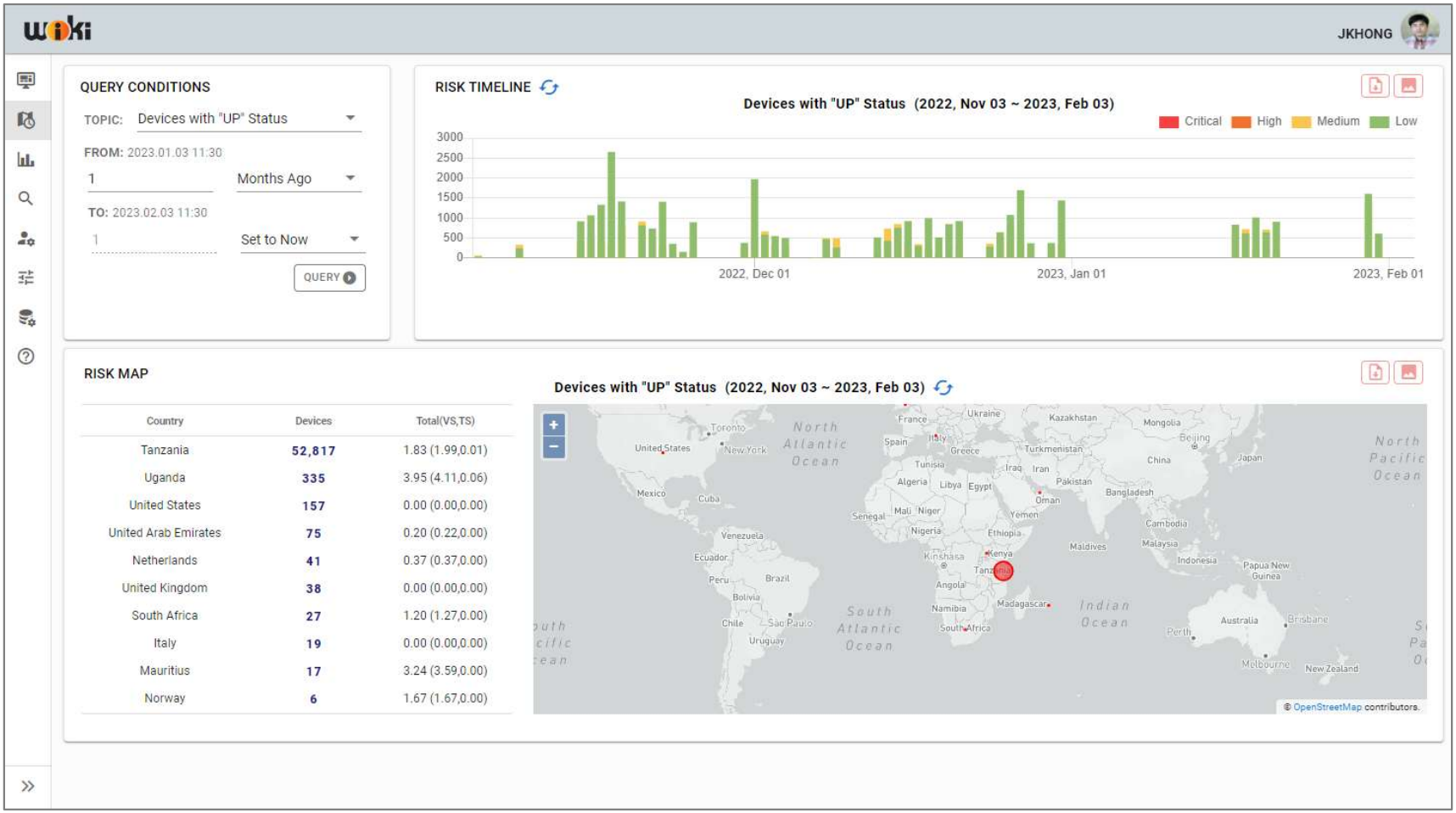
- 이 메뉴는 사용자가 알아야 하는 중요 정보들을 요약하여 제공한다.
- 이 메뉴를 통해, 사용자는 현재 보안위험 수준, 시계열 관점의 위험도 추이, 위험도 Top10 Devices 현황, Top 통계정보 등을 한눈에 알 수 있다.



Copyright © 2022 WiKi Security Corporation All rights reserved

Menu: Timeline

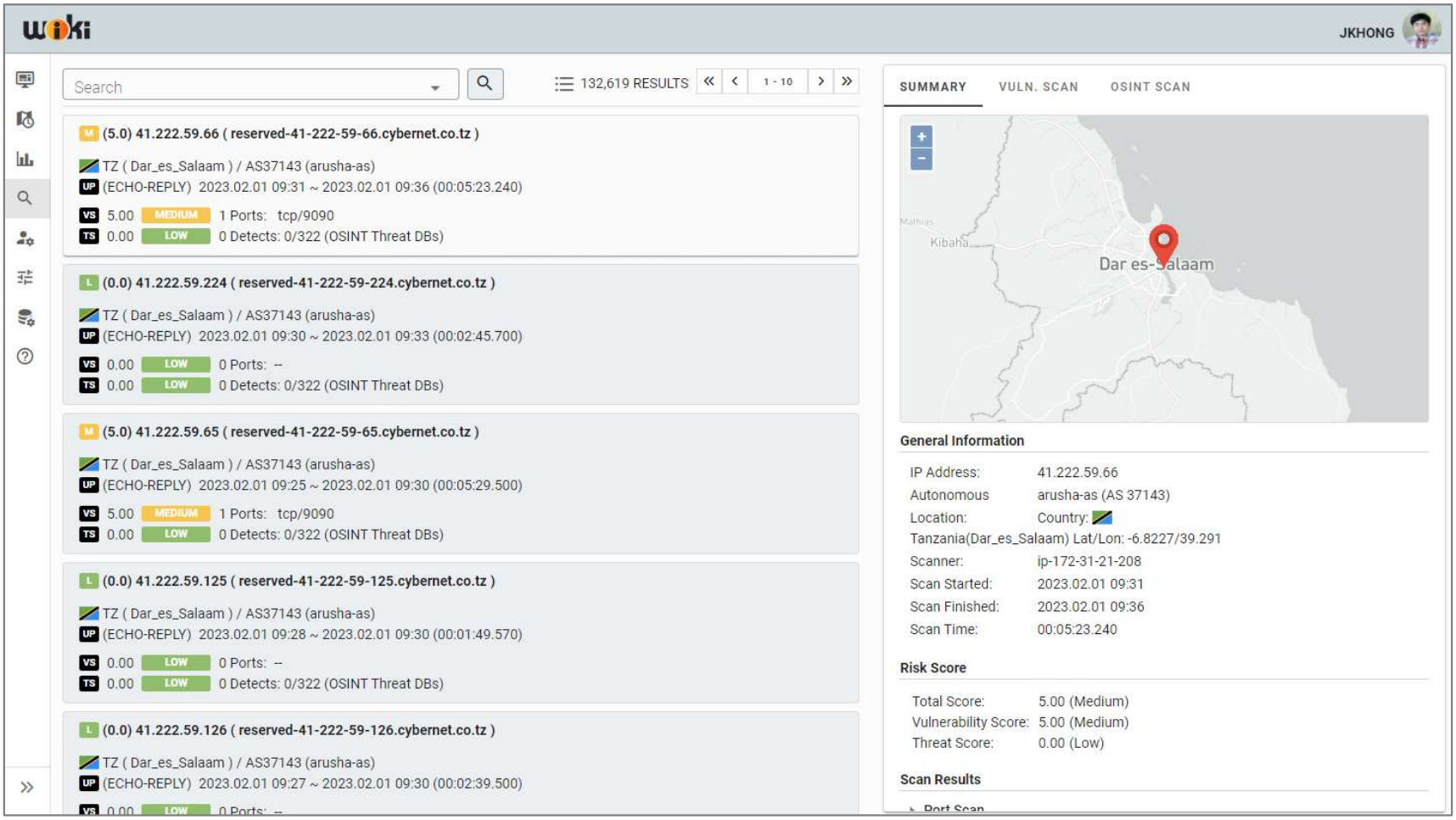
- 이 메뉴는 시계열 관점과 지리적 관점에서 사용자가 주의깊게 관찰해야 하는 상태를 제공한다.
- 이 메뉴를 통해, 사용자는 주어진 조건 검색을 활용하여 시계열 관점과 지리적관점에서 스캔결과들을 다양하게 조회할 수 있다.



Copyright © 2022 WiKi Security Corporation All rights reserved

Menu: Search

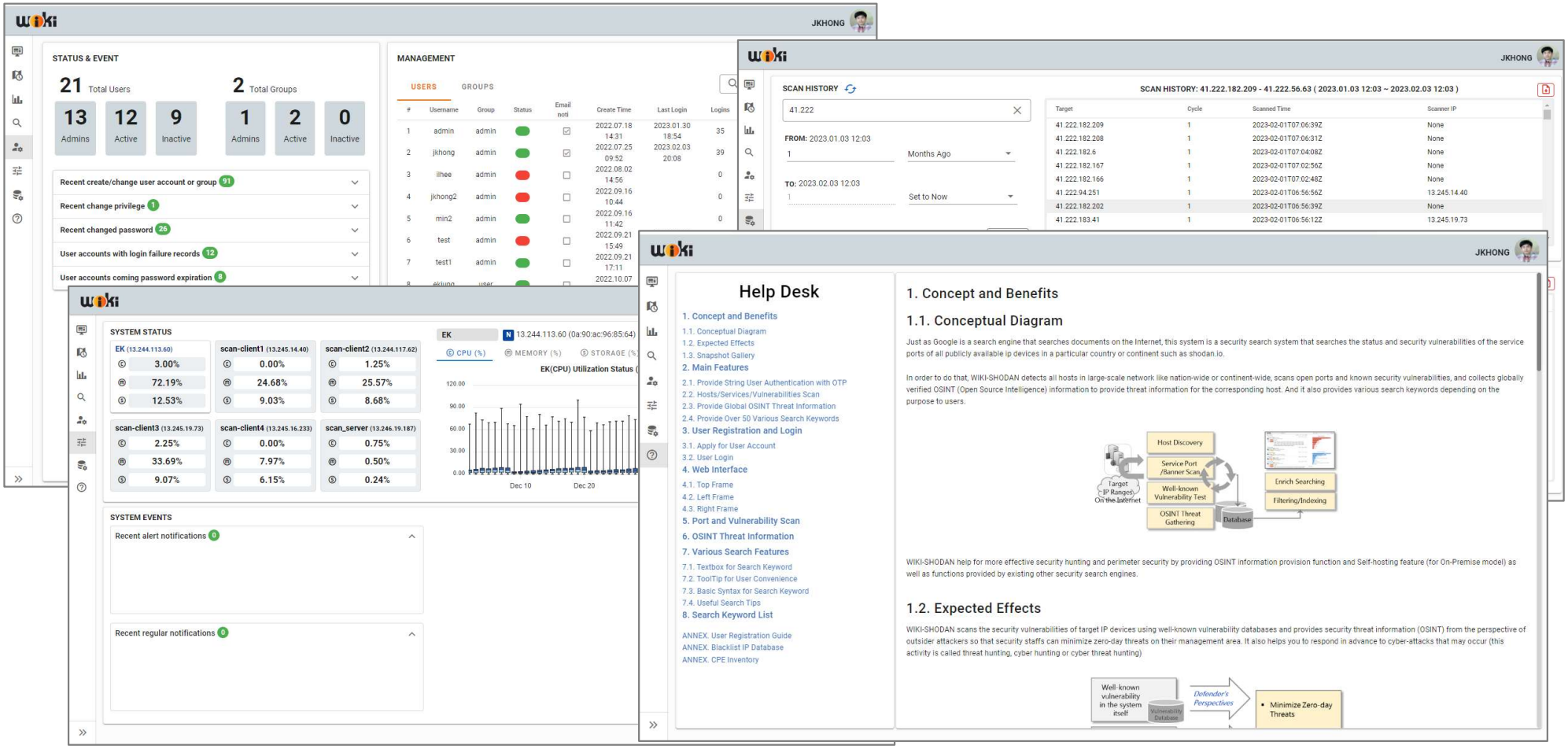
- 이 메뉴는 검색어를 이용하여 IP device의 상세한 정보를 검색할 수 있는 기능을 제공한다.
- 사용자는 시스템이 제공하는 60개 이상의 다양한 검색 키워드를 이용하여 개별 IP device의 AS name, 지리적 위치와 같은 일반정보부터 상세한 취약점 스캔결과, Threat 스캔결과 등을 검색할 수 있다.



Copyright © 2022 WiKi Security Corporation All rights reserved

Menu: User&Group, System, Configuration, Help

- 이 메뉴들은 시스템관리자가 사용자 계정, 서버들의 상태 등을 관리하기 위한 기능을 제공한다.
- 관리자는 이 메뉴를 통해 사용자계정을 생성/변경/삭제할 수 있으며, 서비스를 구성하는 서버들의 Health check, 백업상태 등을 관리할 수 있다.
- Help 메뉴는 사용자와 관리자에게 필요한 시스템설명, 검색키워드, CPE 등을 제공한다.



ANNEX - PRODUCT MODELS

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