SABA SAMANEH
www.sabasamane.com

NET.AUDIT-Network Equipment Testing System
Network Equipment Security Configuration Testing System

Product Description

Improper configuration of active network equipment, such as routers and switches, can be one of the weaknesses in computer networks that may lead to security bottlenecks. This, in turn, can increase an organization's exposure to cyber-attacks!
The way network equipment is configured serves as the basis for implementing the concept of defense in depth and designing a multi-layer security architecture, which is recognized as a successful approach in cyber defense!

One issue is that organizations are often hesitant to grant access to private sector firms and security experts to inspect their network. In some cases, the organization may be unable to provide such access due to its mission and information classifications. Consequently, the internal network remains untested and unaudited, relying solely on the knowledge of the organization's internal network team.
Proper configuration of the network infrastructure can decrease the likelihood of intrusions into all parts of the organization, making it more difficult for viruses, ransomware, or hackers to attack from within.
The forthcoming product will evaluate the setup of active network equipment, including routers, switches, firewalls, and others. Upon receiving the configuration file, it will conduct a security audit using checklists and identify any non-compliance issues with international standards.

This product can function independently of the organization's internal network and the Internet. It only requires the configuration files of the equipment to be loaded into the system, and the audit is then conducted based on that information.

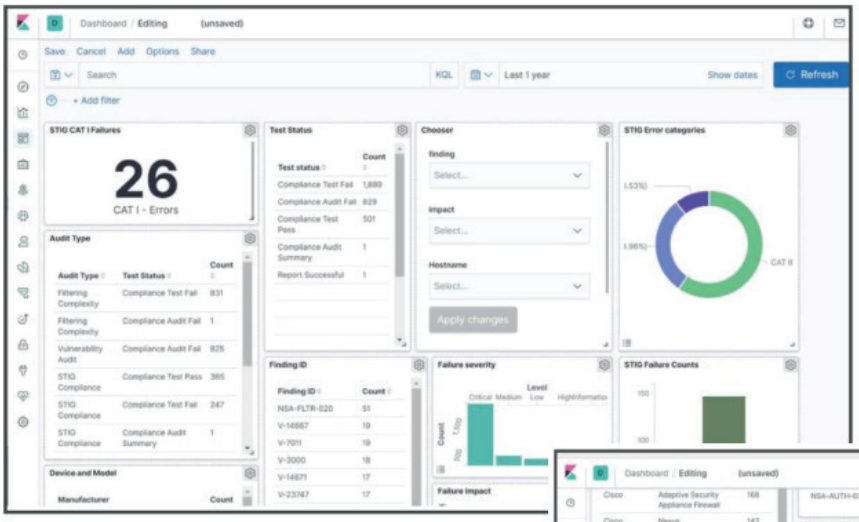
Technical specifications

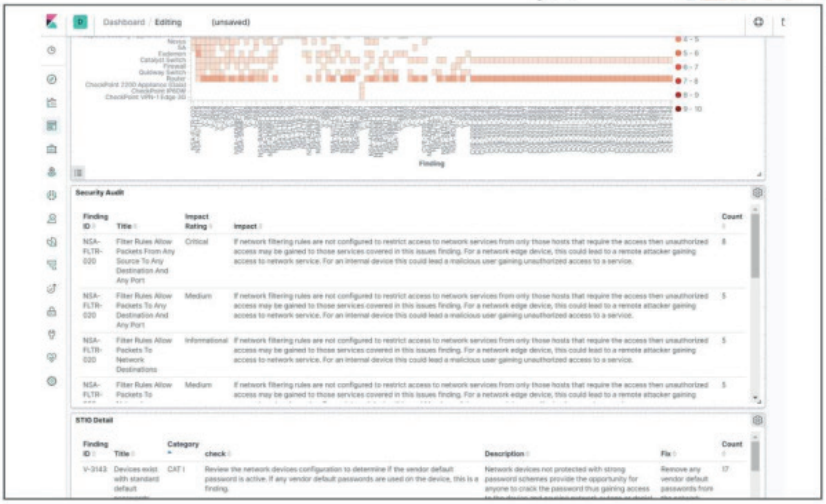
Server specifications	VMWARE SEX/XEN
Web interface specifications	NodeJS
Windows interface specifications	C#.Net
Language interface specifications	Persian-English
Types of services	Evaluation of the security of active network equipment configuration

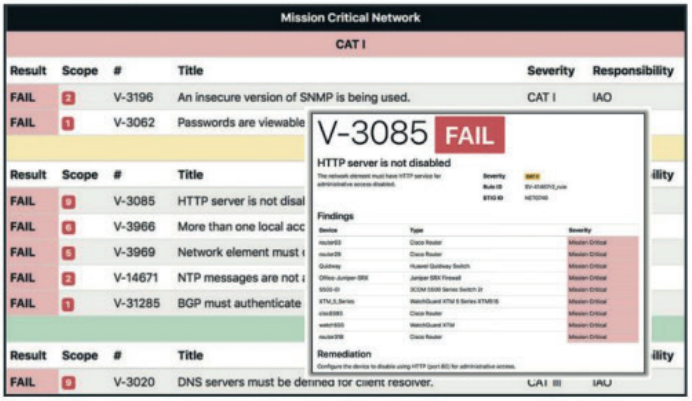
Other system capabilities and features

Management panel	Windows-based Web-based
User interface language	Persian-English
Software architecture	Client-server
Other facilities	✓ The system enables automated evaluation of network equipment, eliminating the need for human intervention. ✓ It generates both technical and management reports, ✓ It provides technical solutions to address any security issues that are identified. ✓ Additionally, it can evaluate up to 100 pieces of equipment in under five minutes. ✓ The system sends regular reports to managers via email
Covered equipment	✓ Cisco ✓ Fortinet ✓ Palo Alto Networks ✓ Netfilter IPTables ✓ 3COM ✓ F5 ✓ HP ProCurve Network ✓ Huawei ✓ Juniper Networks, etc.
Covered standards	1- The NIST 171-800 standard is met by over %80 of the requirements. 2- Over %90 of the requirements in the NIST 800-53 standard are satisfied. 3- More than %80 of the PCI DSS standard's requirements are met. 4- Over %90 of the security checklists' requirements are fulfilled.
Hardware architecture	The system requirements for the server include an Intel processor with a minimum of 4 cores, a RAM capacity of at least 16 GB, a storage capacity of at least 2 TB, and two network interfaces.

Integration of system output with ELK







Some of Our Customers

Asan Pardakht Persian Co.

Tourism Information Technology Development (TIT) Co.

Hajj & Pilgrimage Organization

Ministry of Roads & Urban Development (MRUD)

Ministry of Industry, Mine, & Trade (MIMT)

Ministry of Agriculture Jihad

Arg Center

Arman Insurance

Bank of Industry & Mine

Road Maintenance & Transportation Organization

Saba Mihan Co.

Arian Negin Kish Co.

Arian Negin Arg

Atin Madan Midia Co.

Institute of Standards and Industrial Research of Iran