Comprehensive Network Security Assessment

CNSA provides visibility into the security posture of your internal and external networks and systems. It is a comprehensive security assessment of your technology environment.

This assessment includes internal and an external vulnerability assessment, manual validation and penetration testing of internal and externally facing networks, systems, sites and applications from a threat actor's perspective.

CNSA also includes identification, manual validation and exploitation of vulnerabilities, along with actionable remediation recommendations for improved security.

In addition to network-based testing, this assessment goes beyond by ensuring that the Return on Investment (ROI) of your infrastructure is maximized from a security adoption standpoint. This is done by verifying that all available and effective security features and controls have been implemented.

Highlights

- Assessment of current configurations
- Network-based vulnerability testing and manual validation
- Comparison against best-practices
- Feature analysis
- Classification of severity of findings
- Remediation recommendations

Targets

- Firewalls
- Routers
- Switches
- Other networking devices
- Configurations
- Security features and capabilities
- Network architecture and topology
- Hosts (server and endpoint)
- Applications and Databases
- Unstructured data

Contact **Shadow Canvas** today for **a free consultation!**

11037 Warner Ave #202, Fountain Valley, CA 92708 | (949) 579-9341 | shadowcanvas.com