CyberCase
Record, Detect, Protect

CODEVALUE

WHITEPAPER

CYBERCASE

ASSESSMENT KIT

THE ULTIMATE SECURITY SOLUTION

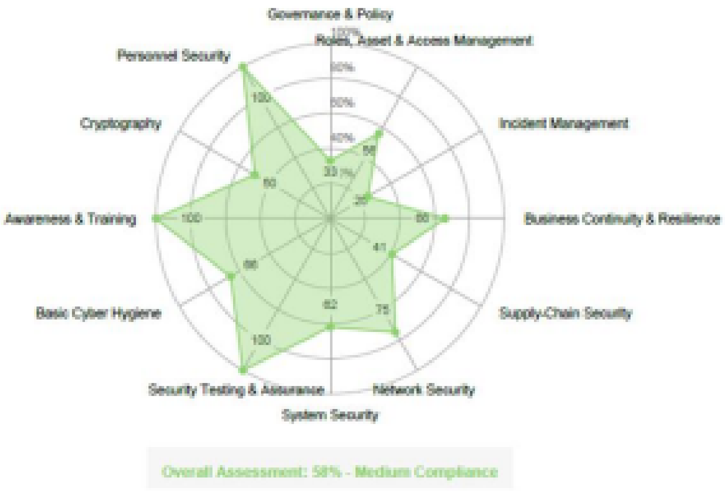
Cybercase redefines security with cutting-edge technology designed to empower cybersecurity teams and network administrators

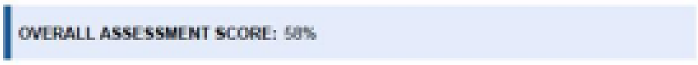
CODEVALUE
www.codevalue.com

The Ultimate Cyber Assessment Solution

CyberCase redefines risk assessment - giving every IT person the capabilities to become an expert security person.

Leveraging multiple tools together to create a smart AI risk assessment report - Summarizing risks and compliance and suggesting mitigations.



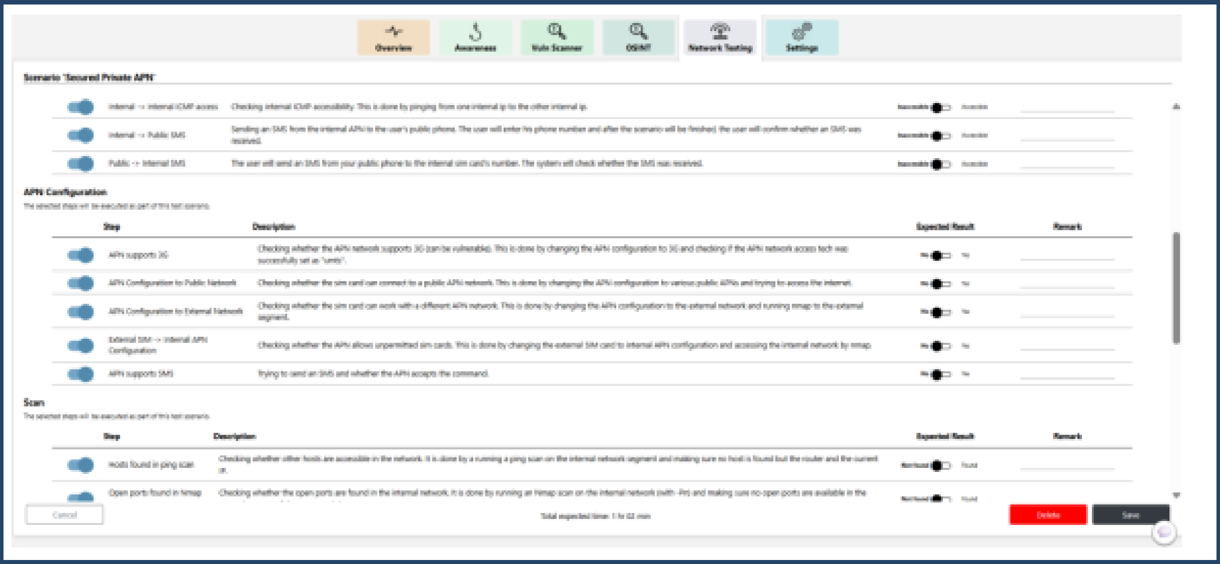


OVERALL ASSESSMENT SCORE: 58%

The Tools :

OSINT Analysis: OSINT automation platform that gathers, analyzes, and visualizes data from hundreds of sources automatically for threat intelligence and digital investigation.
Vulnerability Scanner: Vulnerability scanner with various protocols and performance tuning for large-scale scans. The scanner obtains vulnerability detection tests from a daily updated feed.
LLM Penetration Testing: Evaluation and red teaming for LLM applications. Scanning for security vulnerabilities, testing quality and accuracy of prompts and models.
Phishing Awareness Campaigns: Simulated phishing campaigns with customized email templates, scheduled launches, and detailed real-time tracking and reporting.

Network Security Analysis: Enhance your network's security with an advanced analysis tool.
Endpoint Security Analysis: Correlate and interpret endpoint and network equipment logs.
Gap Analysis: AI-powered analysis of security data to identify gaps, provide actionable insights, and recommend remediation steps based on findings from all assessment tools.
Network Hardening Testing: Testing the hardening for different types of networks, accessibility, scanning and performance for both ethernet and APN networks.



Scenario 'Secured Private APN'

Internal -> Internal ICMP access	Checking internal ICMP accessibility. This is done by pinging from one internal ip to the other internal ip.	Inaccessible ● Accessible	
Internal -> Public SMS	Sending an SMS from the internal APN to the user's public phone. The user will enter his phone number and after the scenario will be finished, the user will confirm whether an SMS was received.	Inaccessible ● Accessible	
Public -> Internal SMS	The user will send an SMS from your public phone to the internal sim card's number. The system will check whether the SMS was received.	Inaccessible ● Accessible	

APN Configuration

The selected steps will be executed as part of this test scenario.

Step	Description	Expected Result	Remark
APN supports 3G	Checking whether the APN network supports 3G (can be vulnerable). This is done by changing the APN configuration to 3G and checking if the APN network access tech was successfully set as "umts".	No ● Yes	
APN Configuration to Public Network	Checking whether the sim card can connect to a public APN network. This is done by changing the APN configuration to various public APNs and trying to access the internet.	No ● Yes	
APN Configuration to External Network	Checking whether the sim card can work with a different APN network. This is done by changing the APN configuration to the external network and running nmap to the external segment.	No ● Yes	
External SIM -> Internal APN Configuration	Checking whether the APN allows unpermitted sim cards. This is done by changing the external SIM card to internal APN configuration and accessing the internal network by nmap.	No ● Yes	
APN supports SMS	Trying to send an SMS and whether the APN accepts the command.	No ● Yes	

Scan

The selected steps will be executed as part of this test scenario.

Step	Description	Expected Result	Remark
Hosts found in ping scan	Checking whether other hosts are accessible in the network. It is done by a running a ping scan on the internal network segment and making sure no host is found but the router and the current ip.	Not found ● Found	
Open ports found in Nmap	Checking whether the open ports are found in the internal network. It is done by running an Nmap scan on the internal network (with -Pn) and making sure no open ports are available in the	Not found ● Found	

Cancel

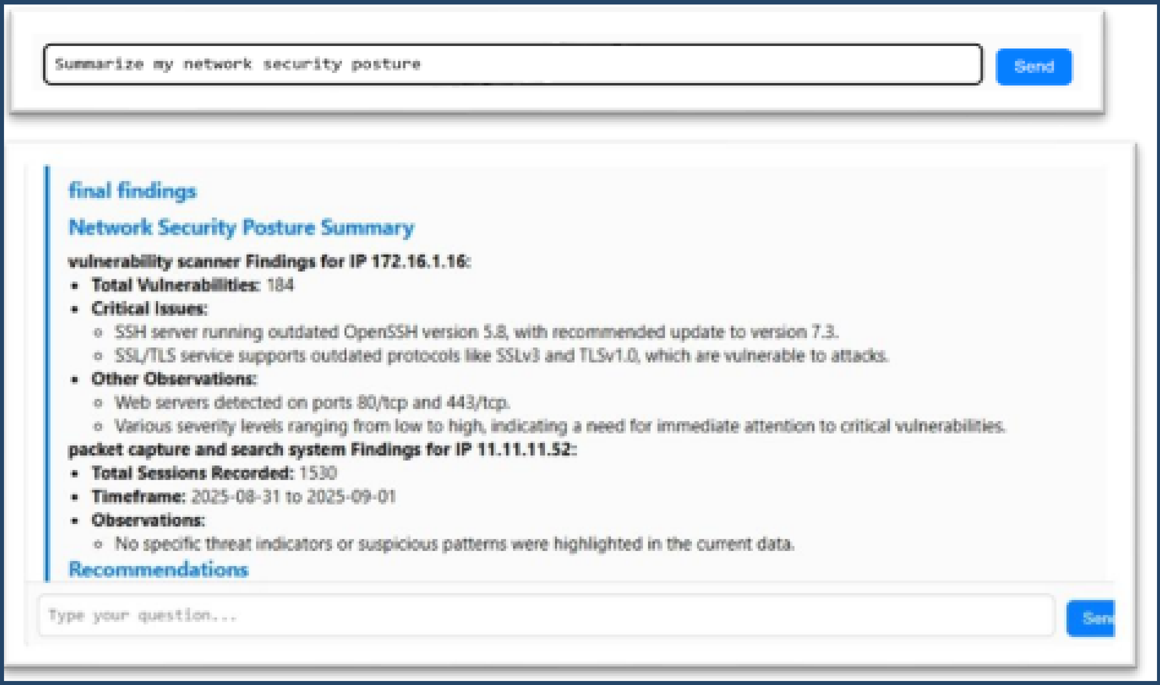
Total expected time: 1 hr 02 min

Delete Save

AI Chatbot

Your Built-In Cybersecurity Assistant

Chatbot and auto-event researcher using a smart AI Agent. Ready to perform any investigation for you while correlating between multiple data sources:



```
Summarize my network security posture
```

final findings

Network Security Posture Summary

vulnerability scanner Findings for IP 172.16.1.16:

- **Total Vulnerabilities:** 184
- **Critical Issues:**
  - SSH server running outdated OpenSSH version 5.8, with recommended update to version 7.3.
  - SSL/TLS service supports outdated protocols like SSLv3 and TLSv1.0, which are vulnerable to attacks.
- **Other Observations:**
  - Web servers detected on ports 80/tcp and 443/tcp.
  - Various severity levels ranging from low to high, indicating a need for immediate attention to critical vulnerabilities.

packet capture and search system Findings for IP 11.11.11.52:

- **Total Sessions Recorded:** 1530
- **Timeframe:** 2025-08-31 to 2025-09-01
- **Observations:**
  - No specific threat indicators or suspicious patterns were highlighted in the current data.

Recommendations

- Revealed abnormal traffic flows and configuration inconsistencies
- Correlated events across network devices and logs
- Identified the root cause of the organization’s recurring networking failures

This allowed the organization to permanently resolve the issue and improve overall network reliability

Why CyberCase Is Different

Plug & Play
CyberCase can be deployed in minutes without installing agents, modifying network architecture, or relying on existing infrastructure**.**

Fully On-Premise & Offline-Capable
All data collection, analysis, and AI-driven investigation can run entirely on-premise. This makes CyberCase suitable for air-gapped, classified, or high-sensitivity environments.

Digital to Physical Unified Security CyberCase correlates network traffic, logs, endpoints, and camera data within a single investigation platform — enabling analysts to connect cyber events with physical-world activity**.**

Built-In AI Investigator
An on-prem AI agent assists analysts by correlating events, identifying anomalies, and accelerating investigations — without exporting data to the cloud**.**

Non-Intrusive Monitoring
Passive traffic capture via network taps ensures zero impact on production traffic and eliminates deployment risk**.**

One Platform for Incidents and Continuous Monitoring
CyberCase supports short-term investigations, breach response, and long-term monitoring with the same platform and hardware.

👉 Request a Demo or Discovery Call

info@codevalue.com
www.codevalue.com