DALIDA | LIRIOS | MENDILLO | OGENA

USER MANUAL

Prepared by
THE SEGURISTA TEAM

Presented for
ELIZER JR. D. PONIO

2025

visit the project

DALIDA | LIRIOS | MENDILLO | OGENA

TABLE OF CONTENTS

visit the project

DALIDA | LIRIOS | MENDILLO | OGENA

TABLE OF CONTENTS

visit the project

THE SEGURISTA TEAM

ABOUT THE PROJECT

Segurista is an innovative Android application designed to detect and prevent network spoofing attacks targeting Internet of Things (IoT) devices. As smart homes and connected devices become increasingly prevalent, the need for accessible cybersecurity solutions has never been greater. Our app provides real-time monitoring, vulnerability analysis, and forensic logging capabilities directly from your mobile device.

Traditional network security tools are often complex, expensive, and require specialized knowledge. Segurista democratizes cybersecurity by offering a lightweight, mobile-based solution that anyone can use to protect their IoT environment. We're closing the security gap between professional-grade tools and everyday users.

Bridging Security Gaps and Creating Impact Through Strategic Innovation

Traditional network security tools are often complex, expensive, and require specialized knowledge. Segurista democratizes cybersecurity by offering a lightweight, mobile-based solution that anyone can use to protect their IoT environment. We're closing the security gap between professional-grade tools and everyday users.

www.reallygreatsite.com

STUDIO SHODWE

WHAT WE DO

Segurista provides comprehensive mobile cybersecurity solutions for IoT environments. Our Android application empowers users to detect, prevent, and analyze network security threats in real-time. We specialize in making advanced network security accessible to everyone, from cybersecurity professionals to everyday IoT device owners who want to protect their smart homes and connected devices.

- **Network Threat Detection**
- **Mobile Security Monitoring**
- **IoT Device Vulnerability Scanning**

Through continuous network monitoring and advanced spoofing detection algorithms, Segurista identifies ARP and DNS attacks before they compromise your devices. Our app performs automated vulnerability assessments, generates detailed forensic reports, and provides actionable security recommendations - all from the convenience of your Android device.

www.reallygreatsite.com

SYSTEM REQUIREMENTS

MINIMUM REQUIREMENTS

- Operating System: Android 9 (API Level 28) or higher
- Special Note: For Android 10+ devices, root access is required for full functionality
- Permissions: Network access and ARP data permissions must be granted
- Storage: Minimum 50MB free space for app installation and logs

NETWORK REQUIREMENTS

- Local Wi-Fi network connection
- Network administrator privileges (for some advanced features)

THE SEGURISTA TEAM

INSTAL LATION

MINIMUM REQUIREMENTS

- Download: Obtain the Segurista APK file from the official source
- Enable Unknown Sources: Go to Settings > Security > Unknown Sources (if installing from APK)
- Install: Tap the APK file and follow installation prompts
- Permissions: Grant all requested permissions when prompted
- Network Access: Ensure Wi-Fi is enabled and connected to your target network

THE SEGURISTA TEAM

APP FEATURES GUIDE

Target Users

- Cybersecurity professionals
- Digital forensic investigators
- IoT device owners concerned about network security
- IT administrators managing smart environments

Getting Started

First Launch and Authentication

1. Splash Screen

- Upon opening Segurista, you'll see the app's branding screen while initial services load.

2. Login Page

Authentication Options:

- Email/Password: Enter your registered credentials
- Google Sign-In: Use your Google account for quick access

New Users:

- Create an account using the registration form
- Verify your email address if required
- Complete initial setup

Troubleshooting Login:

- Ensure internet connection is active
- Check email/password accuracy
- Try Google Sign-In as alternative

www.reallygreatsite.com

THE SEGURISTA TEAM

CORE APPLICATION PAGES

Segurista includes the following main features accessible through different app pages:

Dashboard Page - Network Command Center

Provides an at-a-glance view of your network security status:

- Real-time Network Status: Current connection status and network health
- Active Threats: Live feed of detected security issues requiring attention
- Detected IoT Devices: Count and status of discovered smart devices
- Quick Actions: Direct access to scanning and monitoring features

Using the Dashboard:

1. Review the network status indicator (Green = Secure, Yellow = Warnings, Red = Threats)
2. Check active threats section for immediate security concerns
3. Monitor IoT device count to ensure all expected devices are present
4. Use quick action buttons to initiate scans or access detailed pages

Scan Page - Real-time Threat Detection

Available Scan Types:

- ARP Spoofing Scan: Detects Address Resolution Protocol manipulation attempts
- DNS Spoofing Scan: Identifies Domain Name System redirect attacks

Running a Scan:

1. Navigate to the Scan page from the dashboard
2. Select your desired scan type (ARP, DNS, or comprehensive)
3. Tap "Start Scan" to begin monitoring
4. Monitor real-time results as they appear
5. Review threat detection indicators and severity levels

Understanding Results:

- Green Status: No threats detected
- Yellow Status: Potential security concerns identified
- Red Status: Active threats requiring immediate attention

CORE APPLICATION PAGES

IoT Device Page - Network Device Discovery

Features:

- Automatic Discovery: Lists all IoT devices found on your local network
- Device Information: Shows device names, IP addresses, and basic details
- Status Indicators: Visual indicators for device security status
- Quick Access: Direct links to detailed device analysis

Managing Discovered Devices:

1. Review the complete list of detected IoT devices
2. Tap any device to access detailed information
3. Note security status indicators for each device
4. Use filtering options to sort devices by type or security status

Device Details Page - In-depth Device Analysis

Available Information:

- Device specifications and network details
- Current security status and configuration
- Vulnerability assessment results
- Port scan results and open services

Running Device Analysis:

1. Select a device from the IoT Device page
2. Review basic device information displayed
3. Initiate "Port Scan" to check for open ports
4. Run "Vulnerability Analysis" for comprehensive security assessment
5. Review results and recommended actions

Security Recommendations:

- Follow suggested mitigation strategies
- Update device firmware if outdated versions detected
- Configure secure settings based on recommendations

CORE APPLICATION PAGES

Report Page - Historical Security Data

Report Types:

- Threat Detection Reports: Historical spoofing attack attempts
- Vulnerability Reports: Device security assessments over time
- Network Activity Logs: Detailed network monitoring data

Using Reports:

1. Access the Report page from the main menu
2. Browse historical scan results and threat detections
3. Filter reports by date, device, or threat type
4. Export reports for external analysis or documentation
5. Use data for trend analysis and security planning

Settings Page - App Configuration and Management

Available Settings:

Account Management:

- View and edit user profile information
- Change password and security settings
- Manage authentication preferences

Notification Preferences:

- Configure alert types and frequency
- Set threat notification levels
- Enable/disable specific alert categories

Scan Configuration:

- Adjust scan frequency and scheduling
- Set scan sensitivity levels
- Configure automatic scan triggers

Cloud Sync Settings:

- Enable/disable cloud backup of reports
- Configure sync frequency
- Manage cloud storage preferences

App Information:

- Version details and update status
- Privacy policy and terms of service
- Technical support contact information

THE SEGURISTA TEAM

TROUBLESHOOTING

Common Issues and Solutions

App Won't Start

- Check Android Version: Ensure device runs Android 9 or higher
- Verify Permissions: Grant all requested network and storage permissions
- Restart Device: Reboot your Android device and try again

No Devices Detected

- Network Connection: Verify Wi-Fi connection to local network
- Permissions: Ensure network access permissions are granted
- Network Restrictions: Check if device restrictions prevent network scanning

Scan Results Incomplete

- Root Access: Android 10+ devices may require root access for full functionality
- Network Permissions: Verify ARP data access permissions are granted
- Firewall Settings: Check if network firewall blocks scanning attempts

Login Issues

- Internet Connection: Ensure stable internet connection
- Account Status: Verify account is active and in good standing
- Authentication: Try alternative login methods (Google Sign-In vs. email/password)

TROUBLESHOOTING

Performance Issues

- Storage Space: Ensure sufficient device storage for logs and reports
- Background Apps: Close unnecessary background applications
- Network Load: Reduce network activity during intensive scans

Advanced Troubleshooting

For Root Users (Android 10+)

- Verify root access is properly granted to Segurista
- Check if root management app is blocking network access
- Ensure root permissions include network monitoring capabilities

Network Configuration

- Configure router to allow network scanning if restricted
- Check if device isolation is enabled on Wi-Fi network
- Verify network supports ARP table access

THE SEGURISTA TEAM

TECHNICAL SUPPORT

Getting Help

- **In-App Support:** Access help documentation through Settings page
- **Documentation:** Refer to this user manual for detailed guidance
- **Community Forums:** Connect with other users for tips and solutions

Reporting Issues

When contacting support, please provide:

- **Android version and device model**
- **App version number**
- **Detailed description of the issue**
- **Steps to reproduce the problem**
- **Network configuration details (if relevant)**

Privacy and Security

Segurista is designed with privacy in mind:

- All network scanning occurs locally on your device
- Personal data is encrypted and securely stored
- Optional cloud sync uses encrypted connections
- Forensic logs can be kept local or synced based on your preferences

www.reallygreatsite.com

THE SEGURISTA TEAM

BEST PRACTICES

Security Recommendations

1. **Regular Scans:** Run comprehensive scans weekly or after adding new IoT devices
2. **Monitor Alerts:** Respond promptly to threat notifications
3. **Update Devices:** Keep IoT device firmware updated based on vulnerability reports
4. **Review Reports:** Regularly review historical data for security trends
5. **Backup Configuration:** Use cloud sync to backup important security data

Optimal Performance

- Scheduled Scans: Configure automatic scans during low network usage periods
- Storage Management: Regularly review and archive old report
- Permission Management: Keep app permissions up to dat
- Network Optimization: Ensure stable Wi-Fi connection for accurate results
-

www.reallygreatsite.com

THE SEGURISTA TEAM

THANK YOU

COM223 | CTAPDEVL

- **Team Lead:** Mendillo, Earl
- **Frontend:** Lirios, Elijah
- **Backend:** Ogena, Cristian
- **Database:** Dalida, Nicko