



CYBERBENCHMARK™

A COMPREHENSIVE CYBERSECURITY VULNERABILITY ASSESSMENT:

The SecuLore CyberBenchmark is a cybersecurity risk assessment built specifically for public safety, based upon FCC, APCO, DHS, NIST and NENA The 9-1-1 Association best practices. Developed by experts in public safety technology and cybersecurity, this in-depth report identifies threats and provides prioritized, actionable recommendations to remediate vulnerabilities and enhance your risk posture.



ELEVATE YOUR CYBER AWARENESS

DETECTION BEFORE EXPLOITATION

- Utilizing SecuLore's proprietary, patented technology, the CyberBenchmark identifies vulnerabilities before cyber criminals can use them against you. SecuLore's team of cyber analysts are armed with experience and expertise in public safety targeted cyber attacks, using this experience to rapidly identify activity that may be an indication of malicious behaviors present in your network.

EFFICIENT COLLABORATIVE PROCESS

- With minimal impact on your resources, it will only take 10 minutes to install the Paladin device. Experts will spend 4-8 hours with your team which includes the initial consultation and final presentation of findings.
- From the time of install the passive network data capture takes 1-2 weeks followed by 2-3 weeks of data analysis performed by our team of experts.

CREATED BY AN INDUSTRY EXPERT

- Tim Lorello, Founder & COB, is a public safety technology expert with over 25 years of industry experience including contributing to the FCC's Task Force on Optimal PSAP Architecture (TFOPA) Report, in addition to the NENA i3 working group creating industry standards.
- CEO Sean Scott serves on the Maryland 9-1-1 Commission and the CSRIC VIII working group.



Together We **CYBER-PROTECT** Our Nation's Critical Infrastructure

WHAT SHOULD YOU EXPECT FROM A CYBERBENCHMARK™?

✓ **An Assessment Tailored to You**

Through an initial consultation SecuLore gains baseline information on your network architecture and cybersecurity goals, allowing us to customize the CyberBenchmark to fit your agency's specific needs.

✓ **Passive Data Capture**

Paladin™, SecuLore's proprietary patented network device captures raw packet data for forensic analysis.

✓ **In-Depth Data Analysis**

SecuLore's comprehensive analytical process follows industry best practices and continually evolves to include the latest threat detection techniques.

✓ **Ongoing Insights**

NIST recommends that assessments be conducted by an independent 3rd party. The FCC recommends all PSAPs complete a risk assessment every 90 days to guard against cyber attacks that could take down public safety networks. SecuLore's CyberBenchmark can help you comply with these recommendations.

✓ **Final Presentation Deliverables Include:**

• **CyberBenchmark Report**

A complete review of the assessment's findings

• **Vulnerability Reports**

Actionable vulnerability remediation recommendations for each network segment captured

• **NIST Risk Analysis Checklist**

A prioritized list of all vulnerabilities discovered based on risk to your agency

• **Key Cybersecurity Policies**

Customized cybersecurity policies specific to your environment

• **Cyber Incident Response Plans**

A recommended action plan to guide your team through a cyber incident

• **Master IP List**

A record of all IP addresses communicating during data capture along with all supporting analysis

YOUR TRUSTED CYBERSECURITY EXPERTS

An innovator in public safety focused cybersecurity, SecuLore is passionate about protecting critical services from cyber criminals.

Led by trusted experts in public safety technology and cyber warfare, our team actively contributes to cybersecurity guidelines and policies for numerous formative organizations.

SecuLore has provided thought leadership, cybersecurity expertise, and subject matter insights for the Federal Communications Commission's (FCC) Task Force for Optimal PSAP Architecture (TFOPA), NENA i3 Working Group, APCO Cybersecurity Training, CSRIC VII, CSRIC VIII, Maryland 911 Commission, the Maryland Sub-Committee for Cybersecurity and the iCert Board of Directors.



NIST 800-53 CA-7 (1) Recommendation
Continuous Monitoring | Independent Assessment

LEARN HOW TO ENHANCE YOUR RISK POSTURE

Contact your **ZETRON** relationship
representative to learn more.



Together We CYBER-PROTECT Our Nation's Critical Infrastructure