



EV CHARGING INFRASTRUCTURE ZERO TRUST ASSESSMENT

UNCOVER THREATS, PREVENT DISRUPTION, AND PROTECT EV CHARGING NETWORKS FROM CYBERATTACKS.

Electric vehicle (EV) ownership in the U.S. is set to grow tenfold by 2030, and the country is gearing up to meet demand. Today, 48,000 public charging stations serve EV owners across the U.S., and the Infrastructure Investment and Jobs Act will add 450,000 more in the next five years. While this rapid expansion is great for EV adoption, it also opens the door to major cybersecurity risks that could disrupt charging networks, compromise data, and even threaten the power grid.

DMI's EV Charging Infrastructure Zero Trust Assessment (ZTA) helps agencies uncover vulnerabilities, keep charging stations running, and protect the people who rely on them. Through penetration testing, we uncover threats like malware, supply chain attacks, and man-in-the-middle exploits, demonstrating tactics such as SQL injections and denial-of-service attacks. Combined with alerts-based threat intelligence and dark web monitoring, DMI's ZTA assessment identifies risks and equips your agency to proactively tackle them.

BUSINESS BENEFITS

Prevent Disruption

Shield the power grid from cyberattacks that could cause blackouts or disrupt vehicle-to-grid (V2G) operations.

Strengthen Security

Identify all hardware, firmware, and software assets, including proprietary and open-source components, while pinpointing vulnerabilities and potential exploits.

Close Security Gaps

Proactively detect and address weaknesses before attackers can exploit them.

Improve Reliability

Keep charging stations trustworthy, reliable, and always available for users.

Safeguard Data

Protect customer data from privacy breaches, financial fraud, and unauthorized access.

Reduce Costs

Lower financial losses, legal fees, and emergency maintenance through proactive risk mitigation.

FEATURES

Asset Discovery and SBOM Mapping

Gain a complete inventory of hardware, firmware, and software assets, including open-source and proprietary components. Ensure nothing slips through the cracks in your cybersecurity strategy.

Human-Led and AI-LLM-Based Penetration Testing

Simulate advanced cyberattacks to identify exploitable weaknesses. Thoroughly analyze threats by combining expert insights with AI precision.

Binary Software Composition Analysis

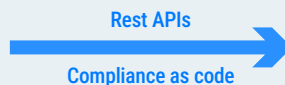
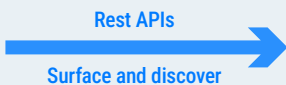
Detect vulnerabilities in software binaries, uncover potential exploits, and secure your systems against emerging threats in the software supply chain.

Security Control and Attack Path Validation

Verify that your defenses are working as need and ensure attackers can't exploit weak points in your infrastructure or bypass security measures.

DMI ZERO TRUST +

Continuous Attack Surface, Posture Management, & Automated Compliance for EV Charging Infrastructure



Penetration Testing/Security Validation

- Asset discovery and SBOM mapping
- Binary software composition analysis
- AI LLM penetrating testing
- Threat intelligence augmentation
- Security control validation
- Attack path and detection validation

Vulnerability Management

- Vulnerability discovery
- Vulnerability verification
- Vulnerability risk prioritization
- Root cause analysis
- Recommend mitigations

Compliance Reporting

- Controls assessment
- XML, JSON, YMAL format of security controls
- AI-enabled predictive mapping of CVEs to controls
- OSCAL compliance automation for SSP, POA&M generation

CONTINUOUS ATTACK SURFACE & POSTURE MANAGEMENT & AUTOMATED COMPLIANCE BENEFITS



Real-time continuous security posture validation



Emulation of real-world attacks and adversary tactics, techniques, and procedures (TTPs)



Security weaknesses mapped to NIST IR 8473 and NIST 800-53r5 controls for compliance



Automated compliance reporting



Engage@DMInc.com
P 240-728-7168

© Copyright, 2025 Digital Management, LLC (DMI)

DO MORE.

CONTACT US TODAY

About DMI

DMI is a leading provider of digital services and technology solutions, headquartered in Tysons Corner, VA. With a focus on end-to-end managed IT services, including managed mobility, cloud, cybersecurity, network operations, and application development, DMI supports Federal and state and local agencies as well as commercial enterprises around the globe. Recognized as a Top Workplace, DMI is committed to delivering secure, efficient, and cost-effective solutions that drive measurable results.

Learn more at www.dminc.com