901 S Bond Street, Suite 203
Baltimore, MD 21231
202-573-9344
www.tcecure.com
info@tcecure.com

CAPABILITY STATEMENT

TCecure empowers clients to build and maintain effective cybersecurity programs.

√ Cybersecurity Program Management & Advisory Services

We provide subject matter expertise to client leadership developing, implementing, supervising, and monitoring their cybersecurity programs. TCecure has developed and implemented security governance and risk management programs for large federal contractors and a local college required to comply with GLBA and the FTC Safeguards Rule. We also developed written policies, procedures, and artifacts for these clients.

√ Security Risk Assessment & Mitigation

We assess our client's current cybersecurity risk posture using industry-standard frameworks and standards. We then develop and implement mitigation strategies to close gaps, reducing vulnerabilities and exposure to risks. TCecure supported DHS and U.S. Army contractors in obtaining authorization to operate (ATO). We have performed assessment and mitigation services for federal agencies and large and small contractors as well.

√ Security Engineering & Software Assurance

We develop, test, and implement security and privacy controls to harden client IT environments and applications against attack vectors, using a variety of industry-recognized tools. TCecure installed, configured, and upgraded multiple platforms, network solutions, and physical and virtual servers for the U.S. Air Force.

√ Continuous Monitoring & Vulnerability Management

We specialize in continuous monitoring, configuration management, and patch management to proactively prevent vulnerabilities. TCecure has provided ISSO and security-focused network/system administration support to the U.S. Air Force.

√ Security Training & Education

We develop and deliver cybersecurity training and education tailored to our client's goals, desired modalities, and the audience. TCecure has provided training courses to the U.S. Army, CMS, DHS, commercial businesses, Maryland colleges, and a local school system.

Contact Us:

Melanie Brennan, President
443-340-5152
melanie.brennan@tcecure.com

Tina Williams-Koroma, Founder/CEO
202-573-9344
tina.williams@tcecure.com

Socioeconomic certifications: Federal WOSB, Maryland SBE/MBE/DBE

NAICS codes: 541690 (primary), 541513, 541519, 541611, 541618

The information in this Capability Statement is proprietary and shall not be duplicated, used, or disclosed outside the intended recipient. This restriction does not limit the intended recipient's right to use such information if obtained from another source without restriction.

Why TCecure?

Knowledge – TCecure's expert staff has decades of experience and industry-recognized certifications in project management and cybersecurity (PMP, CISSP, CIPP, CDPSE, CompTIA Security+, etc.).

Experience – For over 9 years, TCecure has provided cybersecurity consulting, solutions, and education to federal and state government, large and small businesses, and academic institutions.

Value Adds – TCecure offers CyDeploy™, an automated tool that tests security updates to identify/prevent operational impact, and CySkills™, a customizable Learning Management System for on-demand training.

Happy Customers –

"TCecure's skills in Cybersecurity Business Analysis… Information Technology practices, Cybersecurity, and Risk Management Strategic Planning services are strong and comprehensive. TCecure is extremely knowledgeable of current events, the cybersecurity landscape, and governmental regulations. They worked well with people at all knowledge levels and communicated effectively." – Maryland college

"TCecure helped [us] save money... They supplied knowledgeable and experienced engineers [who] were proactive in identifying and resolving possible issues… All due dates were met or exceeded… [They] maintained excellent communication." – Large federal contractor

"TCecure has been a trusted partner on this program for more than five (5) years… They are communicative, responsive, and their personnel are highly valued by the Government customer. They meet deadlines, and correct any issues identified." – Large federal contractor

Why now?

In 2022, the average cost of a data breach was almost **$6 million** in the financial sector, the second highest of any industry[i].

Verizon reported over **1800 cyber incidents** against financial and insurance companies, 480 with confirmed data disclosures. **77% of breaches** were caused by basic web application attacks, miscellaneous (human) errors, and system intrusion. **66% of threat actors** were external, while 34% were internal[ii].

IBM Security X-Force reported **18.9% of incident response cases** occurred in the finance and insurance sector, making it the second most attacked industry in 2022. The top infection vectors were spear phishing and exploitation of public-facing applications[iii].

Regulatory data security requirements are **complex and evolving**, including FTC Safeguards Rule updates effective in 2023 and Congress exploring a unified and modernized legislative framework[iv].

[i] IBM Security. Cost of a Data Breach Report 2022. https://www.ibm.com/downloads/cas/3R8N1DZJ.

[ii] Verizon. 2023 Data Brach Investigations Report. https://www.verizon.com/business/resources/T5b2/reports/2023-data-breach-investigations-report-dbir.pdf.

[iii] IBM Security. X-Force Threat Intelligence Index 2023. https://www.ibm.com/downloads/cas/DB4GL8YM.

[iv] Congressional Research Services. Banking, Data Privacy, and Cybersecurity Regulation. February 24, 2023. https://crsreports.congress.gov/product/pdf/R/R47434/2.

The information in this Capability Statement is proprietary and shall not be duplicated, used, or disclosed outside the intended recipient. This restriction does not limit the intended recipient's right to use such information if obtained from another source without restriction.