

About the Company



Base10 Technology has a proven track record of delivering innovative services and solutions to the Intelligence Community. Our expert technicians excel in designing secure, obfuscated communications systems and developing advanced AI/ML analytics for both edge and centralized data environments.

Unique Entity ID: YTL4RZ4SYZY7
Cage Code: 9D7N4
NIACS: 541512. 541511.
541519. 541330.
541715. 611420.

Top Secret Facilities Clearance
CMMC 2.0 Level 2 – Self Attestation
Small Business Certified

203 Saint Marys Rd
Essex, MD 21221-1540, USA
www.base10tech.com

Zachary Blazer, CEO
zblazer@base10tech.com

Jarod Simmons, COO
jsimmons@base10tech.com

Core Capabilities:

- Design and implementation of robust, highly resilient, modular, and secure network architectures for high-stakes and high-bandwidth environments.
- Secure utilization of commercial communications for in-field collection networks including commercial internet, Starlink, and local LTE/5G comms.
- Communications monitoring, intrusion detection, and intrusion prevention.
- Large-scale crypto key management.
- Network Monitoring, Intrusion Detection, and Prevention with Tools Like Wireshark, Splunk, and Elastic.
- AI/ML Implementation for large scale dataset analytics as well as preliminary on-site data processing models.
- Automation of data flow processes to prioritize, manipulate, and store unstructured data streams.
- Kubernetes Scaling and ArgoCD for Multi-Organization Core Services and Continuous Deployment.
- Enterprise and black-bag forensics.

Past Performance

Performed work for MPO customer
TS SCI Full-Scope Employees

Implemented commercial internet-based communications via DISA for 3rd party partners, reducing customer costs while simultaneously increasing network path resiliency and security.

Implemented largely automated security and sustainment systems for RMF & STIG compliance in air-gapped and intermittently connected environments, reducing overhead.

Implemented and deployed SD-WAN into a globally distributed network architecture to increase resiliency and network visibility for in-field collection systems.

Engineered AI workflows at the terabyte-scale, using multi-agent funneling and prioritization to generate alerts from real-time analytics, reducing manual review of critical insights.

Developed enterprise monitoring systems with advanced analytics and alerts to identify insider threats and prevent unauthorized data exfiltration from critical environments.

Established specialized laboratory for testing undetected data exfiltration methods, bolstering red/blue team strategies using custom hardware and firmware.