Mark Marsh
4400 STATE HWY 121 STE 300-1265
LEWISVILLE, TX 75056 USA
mark@msmnetsecurity.com
(312) 952-8900
www.msmnetsecurity.com

COMPANY DATA

CAGE Code	8CDL5
UEI Number	WCFDLHXL5KL8
GSA SIN (Cybersecurity)	54151HACS
GSA MAS	#47QTCA22D006Q
SBA 8(a)	EXP: 03/23/2030
STARS III	#47QTCB22D0526
SAM Registration	Active
Disaster Response	Yes
Government P-Card	Yes
Illinois BEP/MBE	Yes

HARDWARE & SOFTWARE SERVICES

Hardware

- IBM z16, POWER and STORAGE
- Palo Alto Cortex XDR and Prisma Cloud Security
- Lenovo NOTEBOOKS & TABLET PCS
- FedRAMP Authorized OT/Endpoint Security

Software

- IBM z/OS
- SECURITY
- VIRTUALIZATION
- UTILITIES Networking
- SW INTEGRATION SERVICES/SUPPORT

541511	Custom Computer Programming Services
541512	Computer Systems Design Services
541513	Computer Facilities Management Services
511210	Computer Software
423430	Computer Hardware
611420	Computer Training
611430	Professional and Mgmt. Training

CORE COMPETENCIES

- AI Governance
- AI Powered OT/IT Cyber Defense
- C-UAS Detection and Mitigation
- Governance, Risk and Compliance (GRC)
- Open Source Intelligence (OSINT)
- IT Staffing and RPO

PAST PERFORMANCE

Fortune 200 Client
Work performed: GRC Software Implementation

Fortune 500 Client
Work performed: SOC Program Development

Fortune 500 Client
Work performed: Global PCI Pre-Assessment

U.S. ARMY CYBER BATTLE LAB (CBL)
Work performed: Cyber Quest 2023

DIFFERENTIATORS

Over 30 years of proven Information Technology industry experience in both private and public sectors.

- Innovative
- Performance Driven
- Flexible

Our focus is working cohesively toward delivering exceptional solutions that outperform client expectations.

- Valued Partner

One company with multiple, independently-rated, best-of-breed services: Cyber Defense/AI Goverance

STAFF CERTIFICATIONS

PCI SSC
- PCIP

ISC2
- CISSP
- CCSP

ISACA
- CISA
- CRISC
- CDPSE
- CISM
- ISACA

CSA
- CCSKv4
- CCAK

GASQ
- ISO/IEC 27001 ISMS Lead Auditor

PMI
- PMP

AWS
- AWS Certified

Red Team Security
- Social Engineering Experiment

CISCO SYSTEMS
- CCNA R&S
- CCDA R&S
- CCNP R&S

TV COMMERCIAL: https://www.youtube.com/watch?v=TM7tV3_fMZI


QPASS™
ARMY FUTURES COMMAND
THREAT DRIVEN
PRIORITY FOCUSED
CONCEPT BASED
FOUNDRY
DATA ENABLED
FUTURES AND CONCEPTS CENTER


QPASS™
ARMY FUTURES COMMAND
THREAT DRIVEN
PRIORITY FOCUSED
CONCEPT BASED
FOUNDRY
DATA ENABLED
FUTURES AND CONCEPTS CENTER
MSMNET NewsWire Press Release

Client: U.S. Army Cyber Battle Lab
Project Scope: Incident Response Playbook Automation Solution Cyber Quest 2023
Exercise: Cyber Quest 2023
Period of Performance 11/01/2022 – 08/01/2023

For nearly ten months, our team planned and integrated our Incident Response Playbook Automation Security Solution (QPASS) into an Army Network as part of the Cyber Quest 2023 (CQ2023) Exercise. CQ2023 involved U.S. and Coalition Cyber Defenders training on our solution.

The U.S. Army wanted a solution that could be learned and deployed quickly to edge networks. Our QRadar Playbook Automation Security Solution (QPASS) allowed for a streamlined response with automation and intelligence. Creating responses x7 faster with dynamic playbooks. Quickly and easily create playbooks with OOTB content and 100's of available integrations. We seamlessly integrated analyst workflow, speeding up investigations and responses. QPASS Streamlined intuitive experience with in-app guidance with drag and drop automation configurations, helping to accelerate the playbook creation process.