VET-CYBER™

The Next Line of Defense

What is **VET-CYBER?**

The landscape and complexity of security has changed tremendously in the last 7 years. EAM Solutions Group LLC has developed a trademarked Cyber Security program called VET-CYBER. VET-CYBER teams are led industry trained cyber security professionals in conjunction with prior military veterans who possess the knowledge of warfare and required tactical skills to eradicate threats & possible vulnerabilities. VET-CYBER is comprised of three components and each component represents the desired level of security and response that a specific client is in search of:

SEAL TEAM- Offensive/Defensive Focused. Customized Security Solutions & Tools, and Full Mitigation Strategy Deployment, Continuous Monitoring, S2EM, Combines actives of SWAT/RECON.

SWAT TEAM- Reactive/Defensive(Threat Extraction) Focused. Removal of Threats and possible hacks. Identification and Investigation of root cause of possible threat/vulnerability, Security Tools, 4Phased Approach to Security, Tactical Approach to Security.

RECON TEAM- Proactive/Defensive Focused. Assessment of Current Polices, Hardware, and Software. Build Recommendations/Strategic Planning (vulnerability road mapping), 4Phased Approach to Security.

Centurion Guard Mode

Centurion Guard Mode- After each team has completed it is respective tasks, post are established. These post are established as monitoring stations. At each post security tools and policies are deployed and continuously monitored for vulnerabilities & possible threats.

The Team

Our teams led by cyber security professionals & trained military veterans...

- Government Security Clearances
- Experience
- Discipline
- Strategic
- Certified
- Detailed

Certifications

- CISM
- CCNA
- CCNP
- CPP
- GSEC
- 8570
- PMP
- ITIL
- CEH
- CISSP
- CompTIA
- Security+
- Networks+

VET-CYBER 4 Phased Approach to Security

Our layered approach to security directly addresses the following key areas:

- Security management,
- Security operations
- Security processes

These key areas are critical to drive comprehensive results and protect your organization (Internal & External)

PHASE 1	• Data Collection- review of current policies, procedures, controls strengths and weaknesses.
PHASE 2	• Network Discovery- collection of network data, vulnerabilities risks and threaths through the running of security tools and methodologies.
PHASE 3	• Data Analysis- review pf collected data (Phase 1-2) to develop increased security policies and improved security awareness.
PHASE 4	• Reporting- documented results of assessment findings (Phase 1-3) and recommend mitigation strategies.