TIER Security and Audit Working Group work priorities

February, 2016

1. Determine standards and frameworks to apply to TIER products and Services (Feb through March, 2016)
    a. Consider impact to regulated data (eg. HIPAA, PCI, etc.) and potential Audit exposure
    b. Consider best practice/industry standard practices (eg. OWASP, BSIMM, CSA, etc.)
    c. Consider industry common standards (eg. NIST, ISO, etc.)
    d. Create standards, framework, and policies review board
    e. Train software developers on approved tools, standards, frameworks, and policies

2. How to ensure the TIER product set is developed securely (March through August, 2016):
    a. Based on standards and/or best practices, consider the following:
        i. Software development lifecycle
            1. Software promotion process
            2. Software delivery process to customers
            3. Develop secure coding standards
        ii. Determine the necessary software development documentation

3. How to ensure the TIER product set is tested securely (March through August, 2016):
    a. Based on standards and/or best practices, consider the following:
        i. Software testing
            1. Adequacy of testing environments
            2. Code testing, pen testing
4. How to ensure the TIER product set is operated securely (March through August, 2016):
    a. Based on standards and/or best practices, consider the following:
        i. Change Management
        ii. Incident/Breach response protocols
            1. Detection
            2. Notification
        iii. Audit evidence and trails
            1. Logging and reporting
            2. Notifications and exception reporting
        iv. Data lifecycle management
            1. Creation, Storage and Retention of information
        v. Vulnerability Management actions
            1. Scanning
            2. Remediation processes and timelines

5. Best practices in engaging TIER products to improve campus Security (Sept 16 through June 17)
    a. Determine metrics and reporting available from/through TIER
        i. Set of KPIs to assure service is working effectively
        ii. KPIs to identify identity/access anomalies
    b. Logging
        i. How to enable log management to support campus security?
            1. Log configuration, dashboards, etc.
    c. Data Analytics
        i. How to leverage TIER data for campus security?
        ii. Data elements to mine
    d. Determine the security relevant documentation necessary to provide to campus contacts