Continuing Security Monitoring and Education for Application Developers

Introduction

Datacap as a company realizes the critical importance of security and privacy in its product development process. Datacap also acknowledges that potential risks to application security evolve rapidly and challenge developers to keep ahead of the newest exploit techniques. A program of continuing education focused on security and privacy issues for application developers is a key tool in keeping Datacap's software products secure and competitive. Datacap encourages and underwrites a variety of continuing education activities for its professional software development staff.

The continuing security education activities are comprised of the following:

- Review latest Microsoft Security Development Lifecycle Core Training classes
- Attendance in Coalfire Systems S-SDLC (Secure SDLC) seminars
- Participating in Microsoft E-Learning Security Clinics and Hands-On Labs
- Encourage recommendations for technical library purchases on security subjects
- Regular review of OWASP (Open Web Application Security Project) website (http://www.owasp.org)
- Regular review of US-CERT (United States Computer Emergency Readiness Team) Current Activity (http://www.us-cert.gov/current/)
- Regular review of SecurityTracker 's Weekly Vulnerability Summary Newsletter distributed via email

Review Microsoft Security Development Lifecycle Core Training classes

Datacap employs the Microsoft Secure Development Lifecycle processes as a core discipline in all if software development and expects all its developers to remain current in the latest SDL processes.

Attendance of Coalfire S-SDLC (Microsoft and other) Security Seminars

Datacap underwrites attendance of development personnel at appropriate security seminars. Emphasis is on security content and presentation because of the emphasis on PCI –DSC, PCI-DSS and PA-DSS. However, relevant presentations by other businesses or organizations with expertise in application security are regularly considered.

Microsoft E-Learning Security Clinics and Hands-On Labs

Datacap underwrites participation and encourages all professional personnel to participate in Microsoft's E-Learning Security Clinics and Hands-On Labs frequently.

Encourage recommendations for technical library purchases on security subjects

Datacap encourages all members of the technical staff to select, review and recommend purchase by the company of relevant books (and other printed or electronic materials) for inclusion in the company's permanent reference collection. Recommended purchases are discussed among staff members at regular and informal meetings for their relevance and usefulness.

Regular review of OWASP (Open Web Application Security Project) website

Datacap encourages all members of the technical staff to regularly visit the website of the Open Web Application Security Project at www.owasp.org. Particular attention to sections related to code development activities is encouraged to provide current perspectives on trends and issues in application security.

Regular review of US-CERT Current Activity

Datacap encourages all members of the technical staff to regularly visit the website of US-CERT (United States Computer Emergency Readiness Team) at (http://www.us-cert.gov/current/) to monitor potential threats to security. Review of this website is encouraged for all members of the technical staff regularly for relevance to NETePay security.

Regular review of SecurityTracker Weekly Vulnerability Summary Newsletter

Datacap subscibes to SecurityTracker's Weekly Vulnerability Summary Newsletter (www.securitytracker.com) and encourages all members of the technical staff to review updates weekly for relevance to NETePay security.