COPYRIGHT

© Crown Copyright, The National Cyber Security Centre 2019. This information is licensed under the Open Government Licence v3.0. To view this licence, visit:

https://www.nationalarchives.gov.uk/doc/open-government-licence/ OGL

When you use this information under the Open Government Licence, you should include the following attribution: CyBOK Version 1.0 © Crown Copyright, The National Cyber Security Centre 2019, licensed under the Open Government Licence: https://www.nationalarchives.gov.uk/doc/open-government-licence/.

The CyBOK project would like to understand how the CyBOK is being used and its uptake. The project would like organisations using, or intending to use, CyBOK for the purposes of education, training, course development, professional development etc. to contact it at contact@cybok.org to let the project know how they are using CyBOK.
The Cyber Security Body of Knowledge

Motivations for Secure Software Lifecycle

Prescriptive Processes

Adaptations of Secure Software Lifecycle

Assess the Secure Software Lifecycle

Vulnerabilities can be exploited without being noticed.

Patching can introduce vulnerabilities.

Customers don't apply patches.

Trusted computing.

SAFECode

Microsoft SDL

Touchpoints

Application Security Control Definition

Design

Secure Coding Practices

Manage Security Findings

Vulnerability Response and Disclosure

Planning the Implementation and Deployment of Secure Development

Manage the Security Risk of Using Third-Party Components

Perform Static Analysis Security Testing

Perform Dynamic Analysis Security Testing

Perform Penetration Testing

Secure Design Principles

Secure Coding Practices

Legal and Industry Requirements

Internal Policies and Standards

Incidents and Feedback

Threats and Risk

Common Criteria

CVSS

Provide Training

Define Security Requirements

Define Metrics and Compliance Reporting

Establish Design Requirements

Perform Threat Modeling

Design and Use Cryptography Standards

Use Approved Tools

Establish a Standard Incident Response Process

SQUARE

KAOS

KPIs

PCI DSS

GDPR

Saltzer Schroeder Principles

IEEE Center for Secure Design Principles

STRIDE

Games for Threat Modeling

Architectural Risk Analysis

Code Review (Tools)

Penetration Testing

Abuse Cases

Risk-Based Security Testing

Security Requirements

Security Operations

Attack Resistance Analysis

Ambiguity Analysis

Weakness Analysis

Human Error

OWASP ASVS

Agile and DevOps

Mobile

Cloud Computing

IoT

Road Vehicles

E-commerce

Use Software Composition Analysis and Governance

Use Tools and Automation

Keep Credentials Safe

Use Continuous Learning and Monitoring

OWASP Mobile Application Security Verification Standard

Mobile Security Testing Guide

Mobile App Security Checklist

Mobile Threat Model

Mobile Application Architecture

Mobile Data

Threat Agent Identification

Methods of Attack

Controls

Multitenancy

Tokenization of Sensitive Data

Trusted Compute Pools

Data Encryption and Key Management

Authentication and Identity Management

Shared-Domain Issues

TPM

SSO

Use of RFID Tags

Default Passwords and Credentials

Use the Manufacturer Usage Description

Develop a Secure Upgrade Process

US National Highway Traffic Safety Administration

IS21434

US Spy Car Act

Intelligent and Connected Vehicles Initiative

PCI DSS

SAMM

BSIMM

Common Criteria

Structural Testing

Methodical Testing

Methodical Design

Semi-Formal Design

Semi-Formal Verified Design

Formally Verified Design

SSL101

KA — October 2019

Page 2