HISOLUTIONS

Know-how to go

Sicherheit in der Softwareentwicklung

Betrieb und Wartung – Sicherheit auch nach dem Release

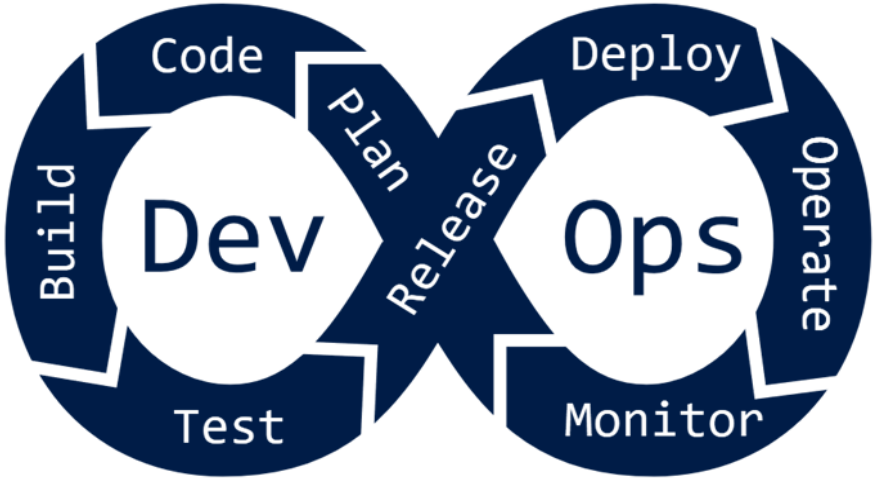
Lutz Weimann

Lutz Weimann

- Fachliche Schwerpunkte:
  - Penetrationstests in den Bereichen Infrastruktur, Web-Anwendungen, Produktprüfung und Mobile Anwendungen (Android/iOS)
- Erfahrungen in der Anwendungsprüfung:
  - Black-Box Reverse Engineering von Android/iOS-Anwendungen
  - Assessments der Anforderungen für mobile Akzeptanzanwendungen nach Mastercard MPOS, Visa mPOS und PCI CPoC

Softwareentwicklung meets DevSecOps

Automatische Sicherheitsscans



Kontinuierliche Prüfung der Container Images

Security Scans wie z. B. Container Scanning

Continuous Monitoring & Incident Response

Sicherheitsrisiken erkennen

- Organisatorische Maßnahmen
  - Schwachstellen Management
  - Change-Prozess
  - Lifecycle Management
- Kontinuierliche Maßnahmen
  - Monitoring der Anwendung/Logfiles
  - Monitoring von öffentlichen Quellen
- Wiederkehrende Maßnahmen
  - Automatische Prüfungen
  - Manuelle Prüfungen

Schwachstellenmanagement

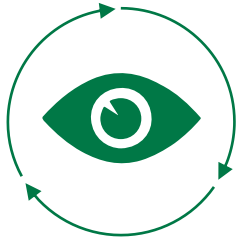
Schweregrad	Bezeichnung	Beschreibung
(C) CRITICAL	Kritische Schwachstelle	Die identifizierte Schwachstel Information über die Schwach Testdurchführung. Für die Schwachstelle existier die die Sicherheit des Untersu
(H) HIGH	Schwerwiegende Schwachstelle	Die identifizierte Schwachstel die Schwachstelle existiert eir die Sicherheit des Untersuchu kann.
(M) MEDIUM	Mittlere Schwachstelle	Die identifizierte Schwachstel die Schwachstelle existiert eir die IT-Sicherheit des Untersuc Umständen gefährden kann. E schwerwiegenden Problem is
(L) LOW	Geringfügige Schwachstelle	Die identifizierte Schwachstel da kein entsprechendes Bedr Steigerung der Sicherheit und Probleme, z. B. in Verbindung Behebung jedoch empfohlen.
(I) INFO	Information	Der identifizierte Sachverhalt erläutert Erkenntnisse aus de haben, aber für den Auftragg (z. B. fehlende Funktionalität)

- Schwachstellenidentifikation
  - Assets/Komponenten/Bibliotheken
  - Informationsquellen
  - Fortlaufende Überwachung
- Schwachstellenbewertung
  - Klar definiertes Bewertungssystem
- Schwachstellenbehandlung
  - Ableitung der Priorisierung aus der Schwachstellenbewertung
  - Fest definierte Vorgehensweisen/Zeitrahmen
  - Tracking der Behebung
  - Nachweise

Schwachstellenmonitoring

- Monitoring von Anwendungen/Systemen
- Öffentliche Quellen
  - National Vulnerability Database (NVD)
  - CVE-Listen
  - Hersteller
- Meldewege für Responsible Disclosure/ Co-ordinated Vulnerability Disclosure

Praktische Prüfung



- Schwachstellenscans
  - (fast) vollautomatisch
  - Identifikation von Low Hanging Fruits
  - Kann automatisiert Versionsstände prüfen, wenn die Komponenten exponiert sind
- Penetrationstests
  - Manuelle Prüfung
  - Prüfung von Business Logik und Schwachstellen mit vielen Abhängigkeiten
- Prüfung von Fremdcode
- Last- und Performance-Tests

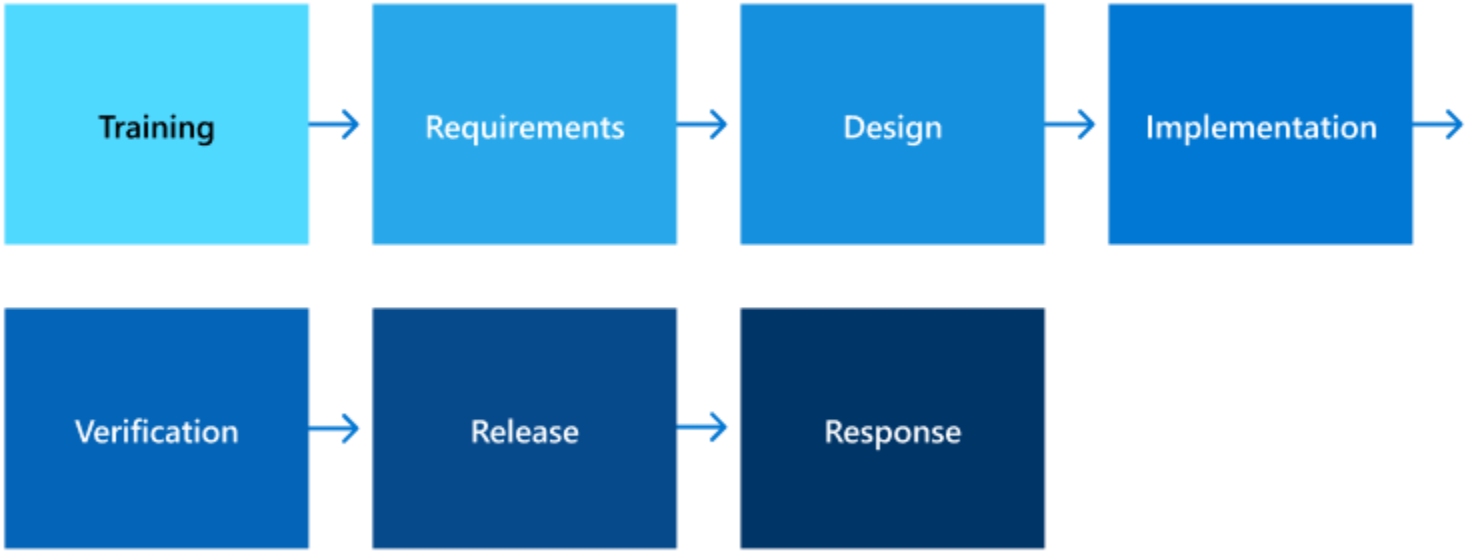
Überwachung von Abhängigkeiten/Bibliotheken

- Software Bill of Materials (SBOM)
  - Liste aller Komponenten und Bibliotheken die eine Software verwendet
  - Erlaubt eine schnell Prüfung ob Schwachstellen in Komponenten/Bibliotheken eine Software betreffen
- Dependency Management Tools
  - Überwachung von Abhängigkeiten
  - Meldung über bekannte Schwachstellen
- Krypo-Kataster/Cryptography Bill of Materials (CBOM)
  - Liste von kryptografischen Methoden
  - Schlüsselmaterial
  - Zertifikate

Härtung / Verantwortlichkeiten

- Installationshandbücher
  - Absicherung der Grundinstallation
  - Liste der Kommunikationsschnittstellen
  - Liste der Services/Prozesse
- Verantwortlichkeiten im Betrieb
  - z. B. Rotation von Schlüsselmaterial/Zertifikaten

Ganzheitlicher Ansatz im gesamten Prozess



Quelle: https://learn.microsoft.com/de-de/compliance/media/assurance-sdl-process-diagram.png

HISOLUTIONS

Schloßstraße 1 | 12163 Berlin

info@hisolutions.com | +49 30 533 289 0

www.hisolutions.com