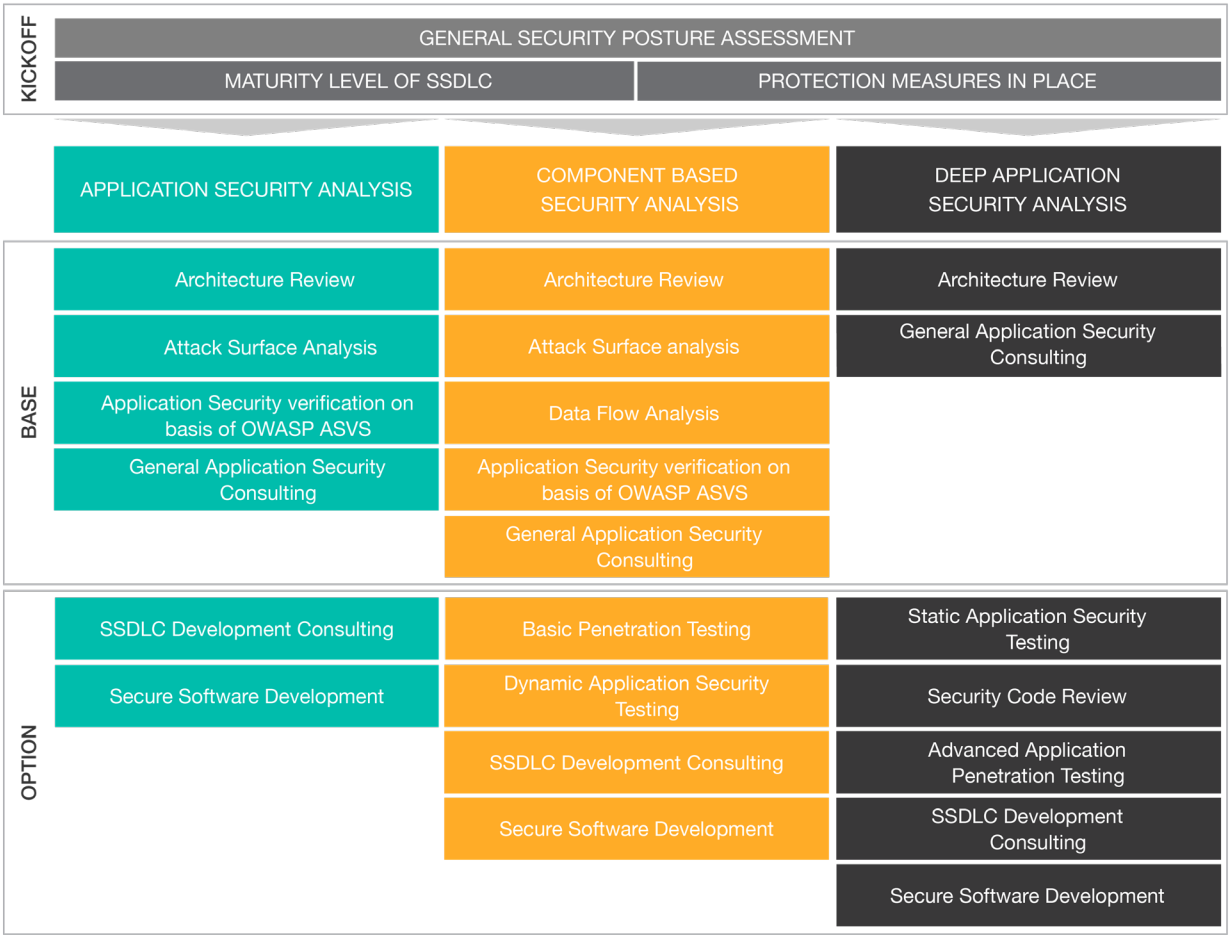
SECURITY SERVICES AG

CLUE

APPLICATION SECURITY CONSULTING



Im Rahmen des Application Security Consulting begleitet Clue Kunden dabei, Massnahmen einzuführen, um die Sicherheit von Software-Eigenentwicklungen nachhaltig zu steigern. Um dies zu erreichen, wird einleitend über ein General Security Posture Assessment beurteilt, welche notwendigen Massnahmen bereits umgesetzt wurden, um eine sichere Applikationsentwicklung zu etablieren. Dies können sowohl Massnahmen im Bereich des Secure Software Development Life Cycles als auch Schutzmassnahmen während dem Betrieb der Applikation sein.

Die nach dem Assessment vorhandenen Ergebnisse dienen dazu, massgeschneiderte Schritte zu definieren, um die Sicherheit der Applikation detaillierter zu bewerten und sie kontinuierlich zu steigern. Clue wählt dabei eine Methodik, welche die involvierten Entwickler befähigt, sichere Software entwickeln zu können.

Klassische Application Security Consulting Dienstleistungen am Markt wählen meist ein Vorgehen, welches mit einem Penetration Testing der Applikation beginnt. Dieses Vorgehen ist jedoch weder nachhaltig noch zielführend. Zwar liegt nach einem Penetration Test ein Schwachstellen-Report vor, die grundlegenden Ursachen, wieso Schwachstellen entstanden sind, werden jedoch nicht behoben. Eine Investition in eine nachhaltig sichere Applikationsentwicklung ist deshalb zielführender und kostengünstiger. Penetration Tests übersehen zudem vielfach eine signifikante Anzahl von Schwachstellen und zeigen deshalb ein verzerrtes Bild der Angriffsoberfläche auf. Im Rahmen eines Application Security Consulting Projektes mit Clue werden Schwachstellen und Design-Schwächen der Applikation ebenfalls aufgedeckt. Es wird jedoch gleichzeitig beleuchtet, wieso diese entstanden sind und wie sie in Zukunft verhindert werden können.

Nach einem einleitenden General Security Posture Assessment wird mit dem Kunden definiert, welche Module aus den Bereichen Application Security Analysis, Component Based Security Analysis oder Deep Application Security Analysis notwendig sind, um die definierten Ziele zu erreichen. Untenstehend befindet sich eine Beschreibung zu den von Clue angebotenen Modulen. Die aus den gewählten Modulen entstehenden Arbeiten, werden anschliessend in regelmässigen

Workshops gemeinsam durchgeführt. Die Projekt-Ergebnisse sind eine nachhaltige Verbesserung der Entwicklungsprozesse, eine nachweisliche Verbesserung der Sicherheit und eine signifikante Reduzierung der Kosten zum Beheben von Schwachstellen in Live-Systemen.

ANGEBOTENE MODULE

SECURITY POSTURE ASSESSMENT

Um einschätzen zu können, welche Schritte bereits in Richtung sicherer Applikationsentwicklung unternommen wurden, wird vorgängig ein Security Posture Assessment durchgeführt. In diesem wird einerseits abgeklärt, welche Phasen/Elemente eines SSDLC (Secure Software Development Life Cycle) bereits umgesetzt wurden und andererseits, welche Schutzmechanismen während dem Betrieb der Applikation bereits etabliert sind.

ARCHITECTURE REVIEW

Im Architecture Review wird die Architektur der im Scope befindlichen Applikation/Komponente analysiert. Dies schafft eine Übersicht aller involvierten Komponenten und Abhängigkeiten.

ATTACK SURFACE ANALISYS

Nach Vorliegen des Architecture Review werden durch eine Attack Surface Analysis alle vorhandenen Angriffsvektoren der im Scope befindlichen Applikation/Komponente dokumentiert und einer Risikobewertung unterzogen.

APPLICATION SECURITY VERIFICATION ON BASIS OF OWASP ASVS

Entsprechend der Risikobewertung aus der Attack Surface Analysis werden alle Komponenten und ihre involvierten Angriffsvektoren einer standardisierten Applikationssicherheits-Verifikation unterzogen. Dies wird auf Basis des OWASP ASVS (OWASP Application Security Verification Standard) durchgeführt, welcher sich als branchenakzeptierter Standard etabliert hat. Der ASVS listet Anforderungen auf, welche eine Applikation erfüllen muss, um resilient vor Angriffen zu sein. Der Standard weist drei Maturitäts-Stufen auf. Die für die Analyse geeignete Stufe wird zusammen mit dem Kunden definiert.

GENERAL APPLICATION SECURITY CONSULTING

Während den Gesprächen und Workshops werden auch Themenbereiche zum Vorschein kommen, welche zu Beginn des Projekts nicht im zentralen Fokus standen, jedoch durch den Projektverlauf neu beurteilt wurden. Diese generellen Applikationssicherheits-spezifischen Themen können in Workshops zusätzlich behandelt werden.

SSDLC DEVELOPMENT CONSULTING

Im SSDLC (Secure Software Development Life Cycle) Development Consulting begleitet Clue Kunden dabei, Massnahmen, Prozesse und Werkzeuge zu entwickeln, welchen ihn dabei unterstützen, einen sicheren und nachhaltigen Applikationsentwicklungs-Prozess zu etablieren.

DATA FLOW ANALISYS

In der Data Flow Analysis wird die im Scope stehende Komponente einer Datenflussanalyse unterzogen. In dieser wird analysiert, wie umliegende Komponenten mit ihr kommunizieren und wie ihr Verhalten im Datenfluss ist. Dies können beispielsweise die Datenflussanalyse des FrontEnds mit einem API-Endpoint sein, oder die Maschinen-zu-Maschinen Kommunikation zweier Container. Die Analyse erlaubt ein genaues Bild über den Kommunikationsaufbau aller angebundener Komponenten. Daraus wird ein Diagramm erstellt, in welchem potenzielle Bedrohungen hypothetisiert aber auch Design Fehler der Business-Logik aufgedeckt werden können.

BASIC PENETRATION TESTING

Im Basic Penetration Testing werden die in der Komponente vorhandenen Angriffsvektoren einem ersten Penetration Test unterzogen. Dieser deckt Schwachstellen auf, welche durch Angreifer mit moderaten technischem Aufwand und Zeit erkennbar wären.

DYNAMIC APPLICATION SECURITY TESTING (SAST SCANNING)

Einige Schwachstellen, welche sich während der Laufzeit manifestieren, können durch entsprechende Werkzeuge in einem DAST Scanning gesucht und aufgedeckt werden.

STATIC APPLICATION SECURITY TESTING (SAST SCANNING)

Durch Static Application Security Testing wird der Source Code der zu analysierenden Komponenten durch entsprechende Werkzeuge auf Schwachstellen und Design-Schwächen untersucht.

SECURITY CODE REVIEW

Sowohl DAST wie auch SAST Scanning weisen keine vollständige Aufdeckungsraten potenziell vorhandener Schwachstellen auf. Einige Schwachstellenkategorien, besonders im Bereich der Business Logik, können nur über einen manuellen Security Code Review entdeckt werden. In diesem wird der involvierte Source Code manuell auf Schwachstellen oder Design-Schwächen untersucht.

ADVANCED PENETRATION TESTING

In einem Penetration Test wird die Applikation und alle involvierten Angriffsvektoren in Laufzeit über ein strukturiertes Verfahren manuell nach Schwachstellen hin untersucht. So können noch verbliebene Schwachstellen, welche in den vorgängigen Analysen unentdeckt blieben, aufgedeckt werden.

SECURE SOFTWARE DEVELOPMENT

Um robuste Sicherheitsmechanismen wie Authentifizierung, Autorisierung, Datenverschlüsselung und Input-Validierung zu implementieren, bietet Clue umfassende Unterstützung in der sicheren Softwareentwicklung. Bei Bedarf arbeiten die Experten eng mit Ihrem Entwicklungsteam zusammen, um die Sicherheit von Anfang an zu gewährleisten.

10.24