Secure Software Development Lifecycle (SSDLC)

AEC

Metodika bezpečného vývoje aplikací šitá na míru

Vyvíjíte aplikace pro sebe nebo své klienty a chtěli byste jim nabídnout bezpečnější produkt? Klíč k bezpečným aplikacím neleží ve větším počtu penetračních testů, ale je ukrytý ve vašem vývojovém procesu. Pouze dobře navržený, měřitelný a opakovatelný proces zajistí vysokou a trvale udržitelnou bezpečnost vašich aplikací. Zavedení metodiky bezpečného vývoje, která definuje bezpečnostní aktivity, role a požadavky od začátku do konce vývojového cyklu je osvědčeným způsobem, jak toho dosáhnout. Ať už o zavedení SSDLC metodiky teprve uvažujete nebo jste již podnikli konkrétní kroky, společnost AEC vám nabízí vytvoření a zavedení metodiky respektující specifika vaší organizace. Za dobu své existence provedl tým AEC stovky penetračních testů, školení a konzultací v oblasti aplikační bezpečnosti a vývoje. Znalosti a zkušenosti tohoto týmu vám budou při implementaci metodiky na dosah.

Služby AEC v oblasti SSDLC

- **Maturity Assessment**
  Provedeme analýzu vašeho procesu vývoje aplikací a vytvoříme přehledný report.
- **Tvorba SSDLC metodiky**
  Navrhneme SSDLC metodiku adresující potřeby a nedostatky vašeho vývoje.
- **Projektová dokumentace**
  Používejte v projektech rychlé a přehledné šablony bezpečnostních artefaktů.
- **Auditní cyklus aplikací**
  Nastavte pro každý projekt auditní cyklus odpovídající business riziku vyvíjené aplikace.
- **Security Awareness Program**
  Vzdělávejte své zaměstnance systematicky v oblasti bezpečnosti za pomoci školení a e-learningů.
- **Pilotní projekt**
  Na skutečném projektu vám ukážeme využití metodiky.

www.aec.cz

Secure Software Development Lifecycle (SSDLC)

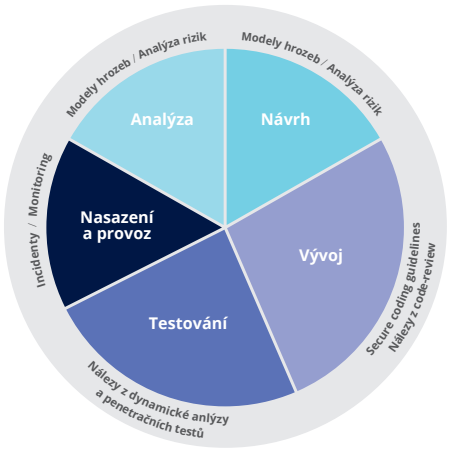
AEC

Důraz na snadnou adaptaci

Každá organizace má jedinečnou kulturu, způsob řízení a nastavení rolí. Aby vaši zaměstnanci SSDLC metodiku přijali, měla by co nejvíce respektovat specifika organizace. V opačném případě hrozí postupné odchýlení od metodiky nebo její zavržení ze strany vývojových týmů.
Námi vytvořená metodika usiluje o plynulou integraci bezpečnostních principů a požadavků do vaší organizace a způsobu řízení projektů. Nemusíte projít náročnou reorganizací procesů nebo rolí, ale rozšíříte kompetence a znalosti příslušných týmů, formalizujete činnosti a dáte jim nové nástroje pro řízení bezpečnosti během vývoje aplikací. Zároveň získáte lepší přehled o stavu projektů díky zavedení nových metrik a důsledného reportingu.

Kompletní pokrytí celého vývojového cyklu

Jistě jste už slyšeli, že náklady na odstranění zranitelnosti nalezené v rané fázi vývoje jsou nižší než náklady na odstranění zranitelnosti nalezené v produkci. V souladu s touto poučkou usiluje většina organizací o zapojení bezpečnosti co nejdříve ve vývojovém cyklu, ale mnoho z nich neumí dále pracovat s bezpečnostními požadavky stejným způsobem jako s funkčními požadavky. Zejména je nedokáží implementovat v souladu se standardy bezpečného vývoje a otestovat pomocí vhodných testovacích scénářů. Naše metodika pracuje s požadavky od identifikace rizik a výběru požadavků až po jejich finální testování.



Braňte se cizím zranitelnostem

Pokud se nevymykáte dostupným statistikám, pak většinu kódu vašich aplikací tvoří přepoužitelný kód třetích stran, knihoven, frameworků nebo kód vytvořený vašimi dodavateli. Vaše kontrola nad vznikem tohoto kódu je omezená, ale případná zranitelnost v tomto kódu ohrozí vaši aplikaci stejně jako zranitelnost vámi vyvinutého kódu. O to důležitější je výběr bezpečných komponent, sledování známých zranitelností a kontrola nad dodavateli. Vyžadujte od svých dodavatelů certifikaci bezpečnosti jejich vývojového cyklu, nebo přesvědčte vaše partery o bezpečnosti vašeho vývoje předložením certifikátu.

Vzdělávejte zaměstnance

Důležitým aspektem SSDLC metodiky je neustálé zvyšování povědomí o zranitelnostech a metodách bezpečného vývoje. Nezapomeňte systematicky zvyšovat kvalifikaci vašich zaměstnanců pomocí našich školení a interaktivních e-learningů.

Přínosy bezpečného vývoje

- Méně nálezů z penetračních testů
- Méně bezpečnostních incidentů v provozu
- Pocit bezpečí pro uživatele
- Nižší riziko ztráty citlivých dat
- Nižší reputační riziko
- Nižší riziko sankcí z nesouladu s legislativními požadavky

Fáze vývoje aplikací

Fáze návrhu

% → Určité procento zranitelností zanesených v průběhu návrhu je odstranitelné analýzou návrhu, modelováním hrozeb nebo vytvářením testovacích případů.

Fáze vývoje

% → Určité procento zranitelností zanesených v průběhu vývoje je odstranitelné při revizi návrhu a odbornými konzultacemi.

Fáze nasazení

% → Určité procento zranitelností zanesených v průběhu nasazení je odstranitelné pomocí revize kódu, statistických analýz, dynamických analýz a bezpečnostního testování.

Cílem je minimalizovat zbylé chyby vedoucí k bezpečnostním zranitelnostem.

Průměrná doba opravy nálezu podle klasifikace závažnosti

Kritický
139 dní

Vysoký
195 dní

Střední
178 dní

Nízký
216 dní

WhiteHat Security Application Security Statistics (2018)

AEC a.s., Veveří 102, 616 00 Brno, tel: +420 541 235 466
AEC a.s., Voctářova 20a, 180 00 Praha 8, tel: +420 226 229 133
AEC s. r. o., Prievozská 6, 821 09 Bratislava, tel.: +421 254 410 283