1.5

# MODEL ZRALOSTI ZABEZPEČENÍ SOFTWARU

## (SOFTWARE ASSURANCE MATURITY MODEL)

**STRUČNÝ PRŮVODCE**

OWASP
Open Web Application Security Project

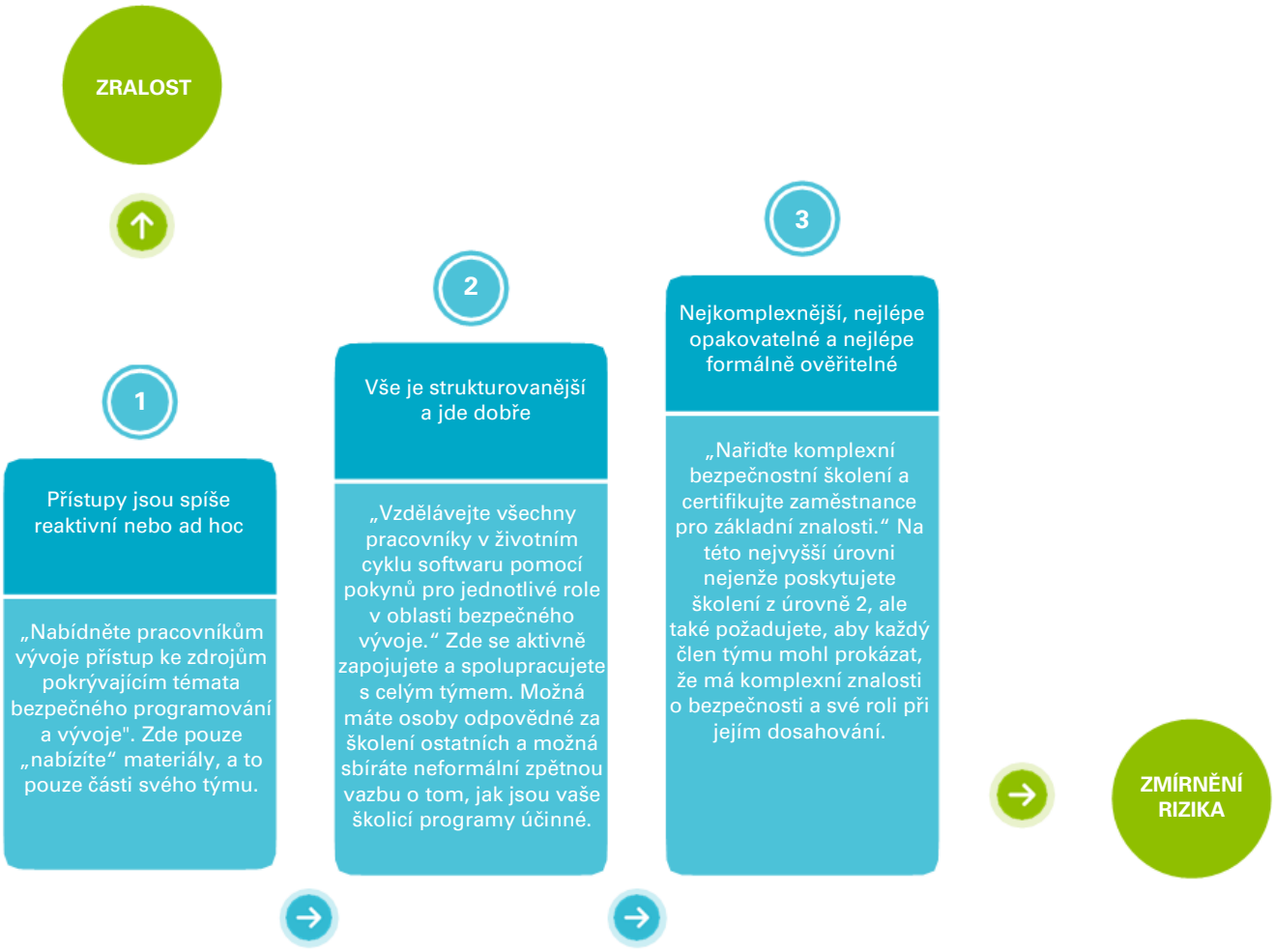
**Lídři projektu:**
**Sebastien Deleersnyder, Bart De Win & Brian Glas**

# STRUČNÝ PRŮVODCE OWASP SAMM

**SAMM (Software Assurance Maturity Model) (Model zralosti zabezpečení softwaru)** je rámec (framework) od OWASP, který pomáhá organizacím posoudit, formulovat a implementovat strategii pro zabezpečení softwaru, kterou lze integrovat do stávajícího **životního cyklu vývoje softwaru (SDLC, Software Development Lifecycle)**. SAMM je vhodný pro většinu kontextů – ať už vaše organizace převážně vyvíjí, outsourcuje, nebo se spíše zaměřuje na pořizování softwaru, nebo ať už používáte vodopádový či agilní model – lze použít stejný přístup. Tento stručný průvodce vás seznámí se základními kroky k zajištění bezpečného softwaru založeného na SAMM.

## POZADÍ

Než se ponoříme do praktických kroků pro rychlý start, popíšeme nejprve stručně samotný model. Model SAMM je založen na souboru 12 bezpečnostních praxí, které jsou rozděleny do čtyř business funkcí. Každá bezpečnostní praxe obsahuje soubor činností, které jsou strukturovány do tří úrovní zralosti (1-3). Činnosti na nižší úrovni zralosti se obvykle provádějí snadněji a vyžadují méně formalizovaných postupů než činnosti na vyšší úrovni zralosti. Níže uvedený diagram to ilustruje na příkladu činností, které se nacházejí v rámci bezpečnostní praxe „Vzdělávání a odborné vedení“ (která je součástí business funkce Řízení (Governance)):




Struktura a nastavení modelu zralosti SAMM jsou vytvořeny tak, aby podporovaly:

i) **hodnocení** současného stavu zabezpečení softwaru,

ii) definice **strategie** (tj. cíle), kterou by organizace měla přijmout,

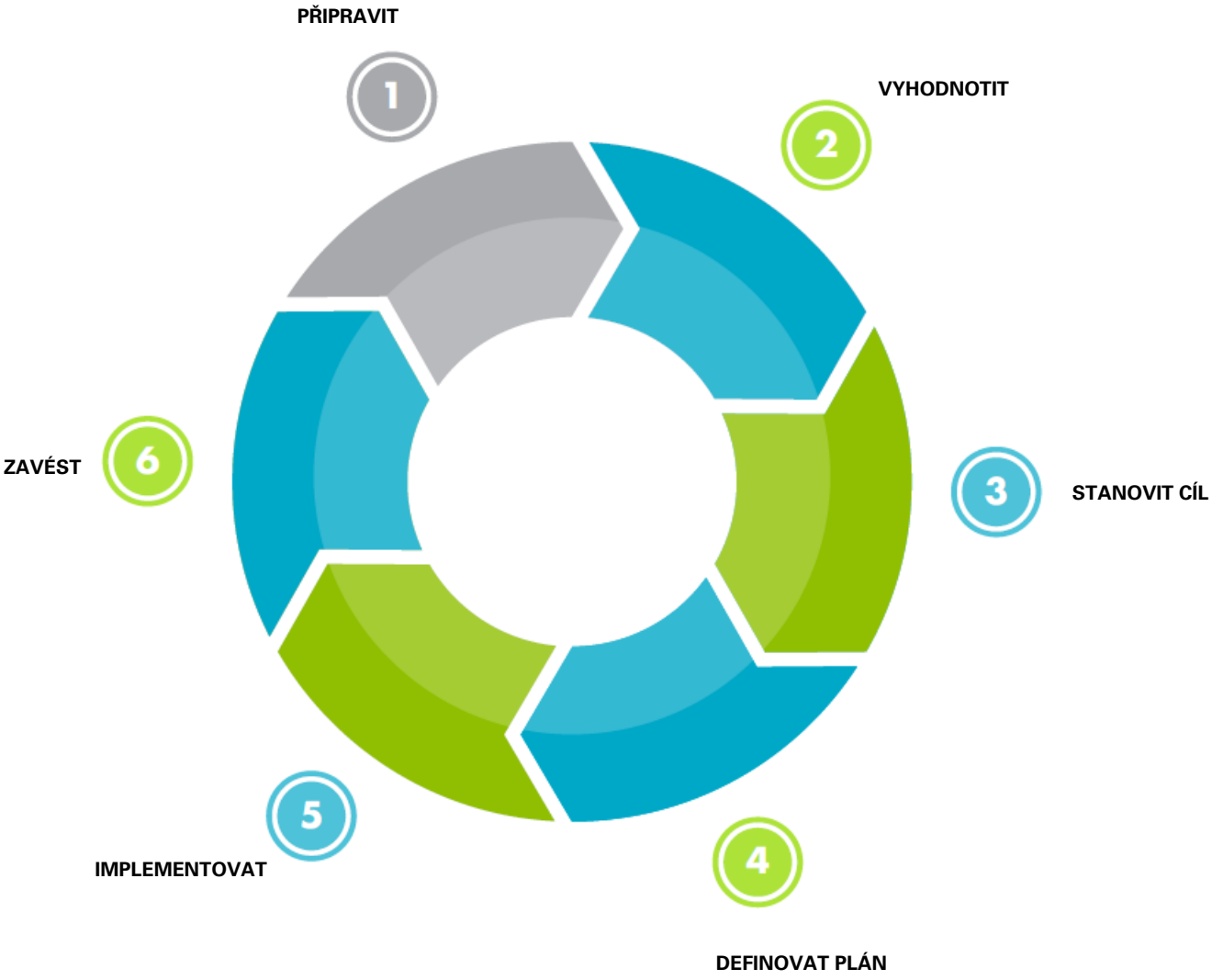
iii) vypracování **realizačního plánu**, jak toho dosáhnout, a

iv) normativní rady, jak **implementovat** konkrétní činnosti.

V tomto smyslu spočívá hodnota **SAMM** v tom, že umožňuje zjistit, kde se vaše organizace nachází na cestě k zajištění softwaru, a pochopit, co se doporučuje pro přechod na další úroveň zralosti. Všimněte si, že **SAMM** netrvá na tom, aby všechny organizace dosáhly úrovně zralosti 3 v každé kategorii. Ve skutečnosti si sami určete cílovou úroveň zralosti pro každou „bezpečnostní praxi“, která nejlépe odpovídá vaší organizaci a jejím potřebám. **SAMM** za tímto účelem poskytuje řadu šablon pro typické organizace, ale doporučuje se je přizpůsobit potřebám vaší organizace.

## JAK TO POUŽÍT?

Následující schéma znázorňuje typický postup použití **SAMM** v organizaci, který začíná přípravou, pokračuje hodnocením, stanovením cíle, plánováním a implementací až po zavedení. **SAMM** je zvláště vhodný pro podporu neustálého zlepšování, v takovém případě se cyklus provádí průběžně (obvykle v periodách 3 až 12 měsíců). Všimněte si však, že není nutné vždy provádět všechny tyto kroky. **SAMM** lze použít například k provedení hodnocení nebo k definování dlouhodobých cílů.



Jak tedy postupovat při realizaci jednotlivých výše popsaných kroků? Na začátek uvádíme následující tabulku, která obsahuje více informací ke každému kroku, pokud jde o cíl, různé činnosti, které je třeba provést, a nejdůležitější podpůrné zdroje:

| KROK | ÚČEL | AKTIVITY | ZDROJE | OSVĚDČENÉ POSTUPY |
|---|---|---|---|---|
|  **PŘIPRAVIT** | Zajistěte řádné zahájení projektu. | **Definujte rozsah**<br>Stanovte cíl úsilí: celý podnik, konkrétní aplikace nebo projekt, konkrétní tým.<br><br>**Identifikujte zúčastněné**<br>Zajistěte, aby byly identifikovány důležité zúčastněné strany a aby byly dobře sladěny s cílem podpořit projekt.<br><br>**Rozšiřte informace**<br>Informujte lidi o iniciativě a poskytněte jim informace, aby pochopili, co budete dělat. | **Zvažte možnost zapojení alespoň:**<br>• výkonného sponzora<br>• bezpečnostního týmu<br>• vývojářů<br>• architektů<br>• business vlastníků<br>• QA testerů<br>• manažerů<br>**SAMM wiki:** https://www.owasp.org/index.php/OWASP_SAMM_Project | • Předběžná kontrola vyspělosti vývoje softwaru, abyste měli realistická očekávání.<br>• Čím menší je rozsah, tím snazší je úkol. |
|  **VYHODNOTIT** | Zjistěte a pochopte zralost zvolené oblasti v každém z 12 praxí zabezpečení softwaru | **Vyhodnoťte stávající**<br>Realizujte rozhovory s relevantními zúčastněnými stranami, abyste pochopili současný stav praxe ve vaší organizaci. Pokud organizaci dostatečně znáte, můžete ji vyhodnotit sami. SAMM poskytuje lehké a podrobné hodnocení – přičemž to druhé je hodnocení založené na důkazech – podrobné hodnocení použijte pouze v případě, že chcete mít absolutní jistotu ohledně výsledků.<br><br>**Určete úroveň zralosti**<br>Na základě výsledků předchozí činnosti určete pro každou bezpečnostní praxi úroveň vyspělosti podle bodového systému SAMM. Činnosti jsou hodnoceny systémem výběru z několika možností a jsou zprůměrovány pro danou oblast bezpečnostní praxe a poté se sečtou pro určení celkového skóre. | **SAMM sada nástrojů:** https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads<br>**Tento zdroj vám poskytne:**<br>• hodnotící otázky<br>• výpočet úrovně zralosti<br><br>**OWASP Model zralosti zabezpečení softwaru:** https://github.com/owasp/ Maturity-Models | • Zajistěte konzistentní hodnocení pro různé zúčastněné strany a týmy pomocí stejných otázek a tazatele.<br>• Zvažte použití různých formátů sběru dat, např. semináře vs. rozhovory.<br>• Ujistěte se, že dotazovaní chápou specifika činností.<br>• Pochopte, které činnosti nejsou pro organizaci použitelné, a zohledněte to v celkovém bodovém hodnocení.<br>• Předvídejte/dokumentujte, zda plánujete udělit částečný počet bodů, nebo jen dokumentujte různá rozhodnutí.<br>• Zopakujte otázky několika lidem, abyste zlepšili kvalitu hodnocení.<br>• Zvažte anonymitu rozhovorů, abyste zajistili jejich upřímnost.<br>• Neberte otázky příliš doslovně. |

| KROK | ÚČEL | AKTIVITY | ZDROJE | OSVĚDČENÉ POSTUPY |
|---|---|---|---|---|
| 3 **STANOVIT CÍL** | Vypracujte si cílové skóre, které můžete použít jako měřítko, jež vás povede k tomu, abyste se věnovali „nejdůležitějším“ činnostem ve vaší situaci. | **Definujte cíl**<br>Stanovte nebo aktualizujte cíl tím, že určíte, které činnosti by vaše organizace měla v ideálním případě realizovat. Obvykle to bude zahrnovat více činností nižší úrovně než činností vyšší úrovně. Jako zdroj inspirace lze použít předdefinované šablony plánů. Ujistěte se, že celkový soubor vybraných činností dává smysl, a zohledněte závislosti mezi činnostmi.<br>**Odhadněte celkový dopad**<br>Odhadněte dopad zvoleného cíle na organizaci. Pokuste se jej vyjádřit rozpočtovými argumenty. | **Předdefinované šablony naleznete v příručce Jak na to (How-To-Guide).**<br>**Pracovní list s plánem postupu podle modelu SAMM (Software Assurance Maturity Model) (součást srovnávacího testu SAMM jako srovnávacího materiálu).**<br>**Využijte pracovní list Roadmap v sadě nástrojů SAMM, který vám pomůže vypočítat zlepšení skóre vyspělosti na základě budoucích odpovědí.** | • Zohledněte rizikový profil organizace.<br>• Respektujte závislosti mezi činnostmi.<br>• Celkový dopad úsilí o zajištění softwaru se odhaduje na 5 až 10 % celkových nákladů na vývoj. |
| 4 **DEFINOVAT PLÁN** | Vypracujte nebo aktualizujte plán, který vaši organizaci posune na vyšší úroveň. | **Stanovte harmonogram změn**<br>Zvolte realistickou strategii změn z hlediska počtu a délky trvání fází. Typický plán se skládá ze 4 až 6 fází po dobu 3 až 12 měsíců.<br>**Vypracujte/aktualizujte plán**<br>Rozdělte realizaci dalších činností do jednotlivých fází plánu s ohledem na náročnost jejich realizace. Snažte se vyvážit náročnost realizace v jednotlivých obdobích a zohlednit závislosti mezi jednotlivými činnostmi. | **Zdroje SAMM:**<br>https://www.owasp.org/index.php/SAMM-Resources<br>**Šablona plánu projektu SAMM:**<br>https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads | • Identifikujte činnosti, které lze rychle a úspěšně dokončit již v počáteční fázi projektu.<br>• Začněte s osvětou / školením.<br>• Přizpůsobte se blížícím se cyklům verzí / klíčovým projektům. |
| 5 **IMPLEMENTOVAT** | Zpracujte plán. | **Provádějte činnosti**<br>Realizujte všechny činnosti, které jsou součástí tohoto období. Zvažte jejich dopad na procesy, lidi, znalosti a nástroje. Model SAMM obsahuje návod, jak to provést. Usnadnit vám to mohou projekty OWASP. | **Užitečné zdroje OWASP pro jednotlivé činnosti jsou popsány na adrese**<br>https://www.owasp.org | • Ke staršímu softwaru přistupujte odděleně. Pokud to není opravdu důležité, nenařizujte přechod na nový software.<br>• Vyhněte se provozním zádrhelům, zejména v případě bezpečnostního týmu. |
| 6 **ZAVÉST** | Zajistěte, aby zlepšení byla k dispozici a efektivně využívána v rámci organizace. | **Propagujte zlepšení**<br>Zviditelněte kroky a zlepšení pro všechny zúčastněné strany pořádáním školení a komunikací se zapojenými subjekty v managementu.<br>**Měřte efektivitu**<br>Měřte přijetí a účinnost zavedených zlepšení pomocí analýzy jejich využití a dopadu. | | • Kategorizujte aplikace podle jejich dopadu na organizaci. Zaměřte se na aplikace s vysokým dopadem.<br>• Využívejte týmové šampiony k šíření nových aktivit po celé organizaci. |

V rámci rychlého startu může první čtyři fáze (příprava, hodnocení, stanovení cíle a definování plánu) provést jedna osoba v omezeném čase (jeden až dva dny). Zajištění podpory v organizaci, stejně jako fáze implementace a zavádění, obvykle vyžadují mnohem více času na provedení.

## ZDROJE OWASP

**V příručce SAMM Quick Start Guide jsou uvedeny odkazy na následující zdroje SAMM:**

- **SAMM wiki:** https://www.owasp.org/index.php/OWASP_SAMM_Project
- **SAMM ke stažení:** https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads
- **SAMM sada nástrojů:** https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads
- **Prohlédněte si SAMM online:** https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Browse_Online
- **Šablona plánu projektu SAMM:** https://www.owasp.org/index.php/OWASP_SAMM_Project#tab=Downloads
- **Zdroje OWASP:** https://www.owasp.org/index.php/Main_Page

Na stránkách OWASP naleznete mnoho skvělých zdrojů, jak SAMM použít. Na wiki OWASP jsme vytvořili sbírku zdrojů SAMM.

Na adrese https://www.owasp.org/index.php/SAMM-Resources najdete všechny naše online zdroje SAMM. Tato kategorie wiki propojuje OWASP a další zdroje s bezpečnostními postupy SAMM.

## ZÁVĚREČNÉ POZNÁMKY

Nejlepším způsobem, jak pochopit SAMM, je začít jej používat. V tomto dokumentu je uvedena řada konkrétních kroků a podpůrných materiálů, podle kterých lze postupovat. Nyní je řada na vás. Srdečně vás zveme, abyste strávili den nebo dva sledováním prvních kroků, pak můžete pochopit a ocenit přidanou hodnotu modelu. Užijte si to!

Návrhy na zlepšení jsou vítány. A pokud máte zájem, zvažte možnost připojit se k e-mailové skupině nebo se stát součástí komunity SAMM.

**Seznamte se se SAMM online – https://www.owasp.org/index.php/SAMM**

**Přihlaste se k odběru e-mailů SAMM – https://lists.owasp.org/mailman/listinfo/samm**

**Sledujte nás na Twitteru – https://twitter.com/OwaspSAMM**