Fortify on Demand

A Micro Focus® Fortify on Demand (FoD) szolgáltatás formájában igénybe vehető alkalmazásbiztonsági megoldás biztonsági tesztelési, sérülékenységkezelési képességeket és szakértelmet nyújt az ügyfeleknek szoftverbiztonsági (Software Security Assurance) programjuk egyszerű létrehozásához, kiegészítéséhez és bővítéséhez.

1. ábra: Fortify on Demand: Biztonság az új SDLC-vel

Három fő ok, amiért az ügyfelek a Fortify on Demand mellett döntenek:

- Rugalmas bevezetés
- Egyszerű használat
- Kiváló eredmények

Főbb termékjellemzők

Nagyvállalati alkalmazások kockázatkezelése

Az alkalmazásbiztonsági kezdeményezések elindításakor fontos első lépés a kockázatok megismerése. A szervezeteknek a szoftverfejlesztési életciklus különböző pontjain törekedniük kell a biztonság kiépítésére. A Fortify on Demand segítségével olyan programot dolgozhatnak ki, amely kiterjed a biztonságos fejlesztésre, az éles indulás előtti biztonsági tesztelésre és az éles működés monitorozására. Az érett biztonsági kezdeményezések a felsorolt területek mindegyikén mélyreható védelmet nyújtanak, de a biztonsági csapat tetszőleges pontról indulhat, és később bővítheti a programot.

A szervezeteknek mind a méretet, mind pedig a komplexitást tekintve gyorsan növekvő alkalmazásportfóliót kell kézben tartaniuk. A régi alkalmazások védelme és az egyedi, illetve nyílt forráskód együttes alkalmazásával, házon belül fejlesztett, új szoftververziók hitelesítése mellett a kiszervezett és a „dobozos" kereskedelmi alkalmazások védelme is kritikus feladat. A külső szoftvereket vásárló ügyfelek esetében a Fortify on Demand forráskódot nem igénylő, egyszerű Vendor Security Management szolgáltatásával a szállító tesztelheti az alkalmazásokat, megoldhatja a problémákat és jelentést készíthet a beszerző számára.

A központosított, online portálon a Fortify on Demandot használó ügyfelek gyorsan megkezdhetik a szolgáltatás használatát, és idővel átfogó szoftverbiztonsági programot építhetnek ki. Az irányítópulton látható a szervezet teljes alkalmazásbiztonsági portfóliója – itt ellenőrizhetők a program kockázatai, korán megoldhatók a kritikus biztonsági problémák, és több csapatra, illetve alkalmazásra nézve rangsorolhatók a javítási feladatok.

Főbb előnyök

Biztonságos fejlesztés

Az alkalmazásbiztonsági problémák korai azonosítása és megoldása a fejlesztés során jóval kevésbé költséges, mint ha erre csak az alkalmazás bevezetése után kerülne sor. Nagyon fontos, hogy a fejlesztők kezdettől fogva lehetőséget kapjanak a biztonságos szoftverfejlesztésre. A fejlesztők által használt integrált fejlesztési környezettel (IDE) tökéletesen összehangolt statikus értékelések azonnali visszajelzést adnak a fejlesztőknek. Az egyetlen egérkattintással hozzáadható nyílt forráskódú komponenselemzéssel elkerülhető a tudottan sérülékeny komponensek hozzáadása. Az auditált vizsgálati eredmények (például a kódsorok részletei és a javításra vonatkozó tanácsok) segítenek kialakítani a kódolás bevált gyakorlatát. A DevOps elveket alkalmazó, fejlettebb szervezetek gyakran a folyamatos építési és integrációs csatorna automatikus lépéseként integrálják

a Fortify on Demand statikus értékeléseit a szoftveres eszközláncba.

Biztonsági tesztelés

A minőségellenőrzési, a teszt- vagy a staging-környezetben futó alkalmazás dinamikus vagy mobil értékelése szimulálja a bűnözők által alkalmazott valódi hackelési technikákat és támadásokat. A webalkalmazásoknál és a webszolgáltatásoknál a dinamikus értékelések automatikus és manuális tesztelési technikákat ötvözve vizsgálják az alkalmazás támadási felületét a kihasználható sérülékenységek azonosítása céljából – még az adott alkalmazáskiadás éles bevezetése előtt. A Fortify ágensével (runtime agent) végzett interaktív alkalmazásbiztonsági tesztelés (IAST) felturbózott dinamikus teszteléssel segít még több sérülékenységet észlelni – és gyorsabban megszüntetni.

A webalkalmazások dinamikus teszteléséhez hasonlóan a Fortify on Demand mobil értékelései is az alkalmazás lefordított binárisával dolgoznak, és automatikus és manuális technikák kombinációjával azonosítják a sérülékenységeket a mobil ökoszisztéma három rétegében – a klienseszközöknél, a hálózatban és a backend-szolgáltatásoknál. Az egyszerű reputáció- és viselkedéselemzésen túlmutató mobil értékelés valódi biztonsági tesztelést biztosít a mobilalkalmazásaik védelmét komolyan vevő vállalatok számára.

Éles működés figyelése

Természetesen nem minden sérülékenység szüntethető meg az összes alkalmazásnál az éles indulás előtt. Az éles környezet konfigurációs hibái pedig újabb, indulás előtt még nem létező problémákat okozhatnak, a kiadási ciklusok között pedig új nulladik napi sérülékenységek jelentkezhetnek. Az éles működés szoros figyelése során a szolgáltatás folyamatosan, dinamikusan keresi a sérülékenységeket és a kockázati profil változásait, felderíti a kártékony alkalmazásokat, valamint futásidőben észleli a biztonsági eseményeket magában az alkalmazásban. A Fortify on Demand egyetlen integrált forrásból biztosítja az éles alkalmazásműködés összes monitorozási tevékenységét.

Főbb jellemzők

Statikus alkalmazásbiztonsági értékelések

A statikus értékelések segítségével a fejlesztők azonosíthatják a sérülékenységeket a bináris, a forrás- vagy a bájtkódban a biztonságosabb szoftverfejlesztéshez. A Micro Focus Fortify Static Code Analyzer (SCA) segítségével végzett statikus értékelések több mint 750 egyedi sérülékenységkategóriát észlelnek a több mint 980 ezer API-t lefedő 25 programozási nyelven. A Fortify on Demand statikus értékelései a biztonsági szakértőink és innovatív Fortify Scan Analytics gépi tanulási platformunk által végzett ellenőrzést is magukban foglalják az álpozitív eredmények kiszűrése és a minőség általános biztosítása érdekében, hogy a fejlesztőcsapatok minél koncentráltabban végezhessék el a javítási feladatokat a szoftver életciklusának korai szakaszában. A Fortify on Demand zökkenőmentesen illeszkedik az ügyfél meglévő agilis vagy DevOps folyamataihoz – „kulcsrakész" integrált fejlesztési környezettel, build szerverrel, a folyamatos integráció képességével és hibakövetési integrációkkal.

Funkciók

- 25 nyelv támogatása: ABAP/BSP, ActionScript, Apex, ASP.NET, C# (.NET), C/C++, Classic ASP (VBScripttel), COBOL, ColdFusion CFML, HTML, Java (Android is), JavaScript/ AJAX/Node.js, JSP, MXML (Flex), Objective C/C++, PHP, PL/SQL, Python, Ruby, Scala, Swift, T-SQL, VB.NET, VBScript, Visual Basic és XML
- Korlátlan fájlméret további költségek nélkül
- Nyílt forráskódú komponensek elemzése (a Sonatype megoldásával)
- Valós idejű sérülékenységazonosítás a Security Assistant segítségével
- Gyakorlatias eredmények egy órán belül a legtöbb alkalmazásnál, DevOps automatizációval.

	Statikus	Statikus+
Alkalmazástípus	Webes, mobil vagy vastag kliens	Webes, mobil vagy vastag kliens
Fortify SCA elemzés	+	+
Nyílt forráskódú elemzés	+	+
Fortify Scan Analytics által végzett automatikus audit	+	+
Security Assistant	+[1]	+[1]
Biztonsági szakértő által végzett manuális ellenőrzés	[2]	+

1 *Csak előfizetéssel*
2 *Csak az első előfizetéses vizsgálatnál*

Webalkalmazások dinamikus biztonsági értékelése

A dinamikus értékelések a valós életből vett, automatikus és manuális hackelési technikákat és támadásokat utánozva, átfogóan elemzik a komplex webalkalmazásokat és webszolgáltatásokat. Az automatikus dinamikus vizsgálatokhoz a Fortify on Demand a Fortify WebInspect megoldást használja. A Fortify on Demand szolgáltatás komplett szolgáltatási élményt nyújt, mivel vizsgálatai a hitelesítési célú makrokészítésre, valamint az eredmények teljes körű szakértői auditálására is kiterjednek az álpozitív eredmények kiszűrése és a minőség garantálása érdekében. Más szállítók nem biztosítják ezt a szolgáltatási szintet. A manuális tesztelés a jól felkészült hackerek által kihasznált sérülékenységtípusokra összpontosít (pl. hitelesítés, hozzáférésszabályozás, adatbevitel validálása, munkamenet-kezelés, üzleti logika tesztelése). Önnek elég megadni egy URL-címet, és csapatunk elvégzi a feladatot.

Funkciók

- Több mint 250 egyedi sérülékenységi kategória azonosítása a webalkalmazásokhoz a QA, a staging vagy az éles működés szakaszában
- Kiterjesztett lefedettség, megnövelt pontosság és javítási részletek az IAST ágens (runtime agent) segítségével
- Tökéletesen integrált támogatás a webhely rendelkezésre állásának fenntartásához vagy a blackout window-k vizsgálatához
- Védelem létrehozása és kezelése az észlelt sérülékenységek alapján az integrált Fortify Application Defenderrel végzett javítás során
- Virtuális patchek generálása valamennyi vezető webalkalmazási tűzfalhoz (WAF).

	Dinamikus	Dinamikus+
Alkalmazástípus	Webhely	Webhely VAGY webszolgáltatások[3]
Fortify WebInspect elemzés	+	+
URL-ellenőrzés és hitelesítés	+	+
Biztonsági szakértő által végzett manuális ellenőrzés	+	+
Interaktív alkalmazásbiztonsági tesztelés (IAST)	+	+
Folyamatos alkalmazásmonitorozás	+[4]	+[4]
Manuális sérülékenységtesztelés		+

3 *Különálló vizsgálatok kizárólag webszolgáltatásokhoz.*
4 *Csak előfizetéssel. Magában foglalja a sérülékenységek és a kockázati profil vizsgálatát; a felderítést külön kell megvásárolni*

Mobilalkalmazások biztonsági értékelése

A Fortify on Demand végponttól végpontig terjedő, átfogó mobil biztonságot nyújt, valós mobilalkalmazás-biztonsági teszteléssel a mobil ökoszisztéma mindhárom rétegében – a klienseszközöknél, a hálózatban és a webszolgáltatásoknál. A webalkalmazások dinamikus teszteléséhez hasonlóan a mobil értékelések is az alkalmazás lefordított binárisával dolgoznak, és ugyanazokat a technikákat alkalmazzák, mint amelyekkel a hackerek kihasználják a mobilalkalmazások sérülékenységeit – legyen szó belső fejlesztésű, kiszervezett vagy megvásárolt alkalmazásokról. Az egyszerű reputáció- és viselkedéselemzésen túlmutató mobil értékelés valódi biztonsági tesztelést biztosít a mobilalkalmazásaik védelmét komolyan vevő vállalatok számára.

Funkciók

- Az iOS- és Android-alapú mobilalkalmazásokat egyaránt támogatja
- Több mint 300 egyedi sérülékenységi kategóriát azonosít a mobil binárisoktól a backend-szolgáltatásokig
- A viselkedés- és reputációelemzés mellett a biztonsági sérülékenységek azonosítására is kiemelt figyelmet fordít
- Fizikai eszközökön végzett manuális tesztelés

	Mobil	Mobil+
Alkalmazástípus	Mobil bináris	Mobil bináris és backend-szolgáltatások
Sérülékenységelemzés (mobil bináris)	+	+
Végponti reputációelemzés	+	+
Biztonsági szakértő által végzett manuális ellenőrzés	+	+
Fortify WebInspect elemzés (backend-szolgáltatások)		+
Manuális sérülékenységtesztelés		+

Folyamatos alkalmazásmonitorozás

Az éles alkalmazások monitorozása egyre gyakrabban jelent kihívást a biztonsági csapatok számára. A Fortify on Demand folyamatos alkalmazásmonitorozó szolgáltatás az alkalmazások felderítését folyamatos, dinamikus sérülékenységvizsgálatokkal és kockázati profilkészítéssel ötvözi egyetlen önálló előfizetéses szolgáltatásban. Az ügyfél teljes alkalmazásportfólióját érintő kockázatokat láthatóvá teszi. Az automatikus felderítő vizsgálatok havonta azonosítják a külső feleknek szolgáltatott, új alkalmazásokat, és a megbízhatósági pontszám feltüntetésével, kockázat szerint rangsorolt listán jelenítik meg az eredményeket (évente max. 12 alkalommal). A megerősített alkalmazások ezt követően az éles működést nem zavaró, folyamatos sérülékenység- és kockázatiprofil-vizsgálatoknak vethetők alá (havonta max. 4 alkalommal). A folyamatos alkalmazásmonitorozás egyrészt ideális első lépés a szoftverbiztonsági (Software Security Assurance) program elindításhoz, másrészt pedig jól kiegészíti a már telepített alkalmazások dinamikus és statikus tesztelését.

Funkciók

- Az alkalmazásfelderítés rutinszerűen azonosít (átlagosan) több mint 3000 webes eszközt a Fortify on Demandot használó ügyfelek számára
- Az innovatív dinamikus vizsgálati motort kifejezetten éles üzemű webhelyekhez optimalizáltuk
- A sérülékenységészlelés azonosítja az OWASP Top 10 lista szerinti leggyakoribb kritikus sérülékenységeket
- A kockázati profil változásának automatikus észlelése és riasztás küldése

Értékelési egység

A Fortify on Demand statikus, dinamikus és mobilalkalmazás-biztonsági tesztszolgáltatásai értékelési egységek vásárlásával és beváltásával igényelhetők. Az értékelési egységek különálló értékelésekre beváltható, előre kifizetett kreditek vagy alkalmazáselőfizetések, amelyekkel a befektetés rugalmasan szétteríthető az egész évre. Az értékelési egységek 12 hónapig érvényesek, és egyenként válthatók be.

Minden egyes értékelésnél vagy előfizetésnél az ügyfelek egy értékeléstípus (dinamikus, statikus vagy mobil) és egy értékelési szolgáltatási szint kombinációját választják. Egy alkalmazáselőfizetés keretében egy alkalmazást mérünk fel korlátlan alkalommal, 12 hónapos időszak alatt. Minden értékelés tartalmaz egy javításvalidálási vizsgálatot az értékelés után legkésőbb egy hónappal.

Értékelés típusa	Különálló értékelés	Alkalmazáselőfizetés
Statikus értékelés	1 értékelési egység	4 értékelési egység
Statikus+ értékelés	2 értékelési egység	6 értékelési egység
Dinamikus értékelés	2 értékelési egység	6 értékelési egység
Dinamikus+ értékelés	6 értékelési egység	18 értékelési egység
Mobil értékelés	1 értékelési egység	4 értékelési egység
Mobil+ értékelés	6 értékelési egység	18 értékelési egység

4. táblázat A Fortify on Demand értékelési egységeinek beváltása

Ügyfélkezelés

Minden fiók hozzáférést biztosít a műszaki ügyfélkezelő csapathoz, akik segítenek ügyfeleinknek az alkalmazásbiztonsági program sikeres megvalósításában. A csapat a Help Centeren keresztül tartja a kapcsolatot az ügyféllel; kezeli a szerződéses ügyeket, a megújításokat és a támogatáskéréseket; továbbá a megoldás alkalmazásának kiterjesztését és az ügyfél sikeres működését szem előtt tartva összehangolja a Fortify erőforrásait, például a rendszer- és folyamatszakértők munkáját.

A Micro Focus Fortifyról

A Fortify a piac legátfogóbb kínálatát nyújtja iparágvezető biztonsági kutatásokkal megalapozott statikus és dinamikus alkalmazástesztelési technológiákból, az alkalmazásokat futásidőben monitorozó és védő megoldásokból. Megoldásai helyben is telepíthetők és szolgáltatásként is igénybe vehetők a napjaink IT-szervezeteinek változó szükségleteit kielégítő, rugalmas és skálázható szoftverbiztonsági (Software Security Assurance) program kialakításához.

További információ:
www.microfocus.com/fod

Kapcsolatfelvétel:
www.microfocus.com

Tetszik amit olvas? Ossza meg.