QUALYSGUARD® POLICY COMPLIANCE

POLICY COMPLIANCE - INFORMACE O STAVU BEZPEČNOSTI A SOULADU S POŽADAVKY — SLUŽBA NA VYŽÁDÁNÍ

Organizace jsou neustále vystaveny nárokům od interních i externích auditorů, aby prokázaly naplnění požadavků v oblasti bezpečnosti ICT. Organizace musí prokázat svůj soulad s různými regulatorními požadavky a průmyslovými nebo bezpečnostními standardy. Jako výsledek musí organizace auditorům ukázat, že je v souladu s předepsanými požadavky v různých oblastech:

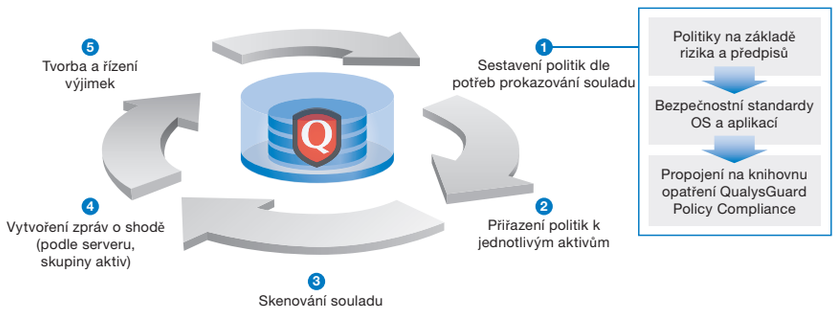
- **Politiky, které popisují, jak organizace realizuje bezpečnost a její integritu.**
- **Důkaz, že politika správně fungovala při auditu v IT prostředí.**
- **Doložit důkazy o případech, kdy byl odhalen nesoulad s požadavky a o provedené nápravě.**

Automatizované řízení zranitelností a shody s bezpečnostními politikami zlepšuje efektivnost organizace, účinně snižuje riziko a poskytuje auditorem vyžadované důkazy o souladu s požadavky.

Představení QualysGuard® Policy Compliance

Modul QualysGuard Policy Compliance rozšiřuje skenovací možnosti služby QualysGuard Vurnerability Management o sběr informací ze serverů a dalších zařízení, o konfiguracích OS a o opatřeních pro řízení přístupu k aplikacím. Tyto informace mapuje na definované politiky tak, aby byla přesně dokumentována shoda s požadavky vyplývajícími z řídící dokumentace, regulatorních předpisů nebo bezpečnostních standardů.

Životní cyklus QualysGuard Policy Compliance



Výhody QualysGuard Policy Compliance

- Kombinované řešení pro skenování zranitelností bez instalování agentů s minimálním dopadem na infrastrukturu ICT.
- Rychlé nasazení díky modelu QualysGuard Software-as-a-Service (SaaS), který nevyžaduje žádnou instalaci nebo správu software.
- Centralizovaný přístup k definování a správě politik konsoliduje množství oddělených procesů do jednoho jednoduchého řešení.
- Volitelné možnosti podpory auditů podle jejich zaměření a v souladu s rozsahem pověření k auditu.
- Kompletní přehled postupů pro přezkoumávání a prokazování souladu.

> *"Není jednoduché ani levné, pro rozsáhlou společnost jako je ta naše, shromáždit informace o stavu bezpečnosti a další konfigurační data pro prokázání souladu. QualysGuard nám umožňuje získávat informace jak o stavu bezpečnosti, tak o shodě ze všech našich celosvětových aktiv ICT. A to vše bez toho, aniž bychom museli instalovat agenty a získávat data přes různé regulatorní nároky a požadavky na soulad.To nám umožnilo razantně redukovat cenu za zprávy o souladu bezpečnosti a navíc jsme získali přesný přehled o naší bezpečnosti a jejím souladu."*

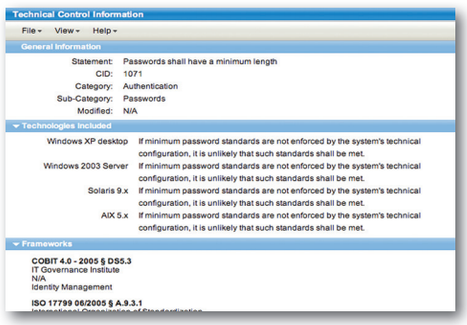
Victor Hsiang, Director of Security Architecture
TransUnion

> *"Regulativy, jakými jsou například Sarbanes-Oxley Act a Basel II, posunuly dosahování souladu do popředí zájmu manažerů. V takovém prostředí musí bezpečnostní manažeři propojovat řízení zranitelností a postupy provádění auditů bezpečnosti do širšího rámce zajišťování souladu a řízení rizik v rámci celé organizace."*

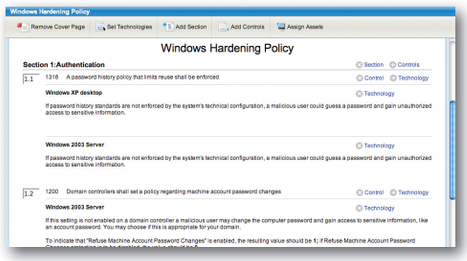
Andreas Wuchner-Bruehl,
Head of Global IT Security
Novartis AG

Vlastnosti QualysGuard Policy Compliance:

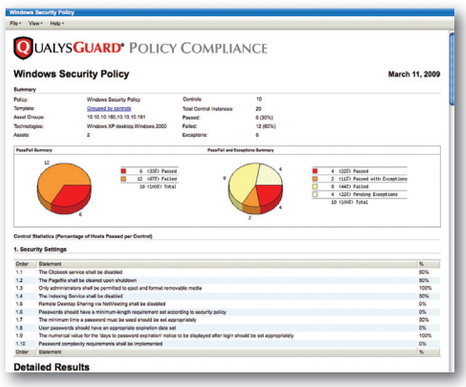
- Automatizovaná kontrola souladu s politikou s využitím stejné infrastruktury, jakou používá QualysGuard pro skenování zranitelností.
- Dostupná knihovna technických opatření je založena na standardech CIS a NIST a obsahuje mapování na standardy jako jsou COBIT, ISO, ITIL,FFIEC, NERC a další.
- Editor pro definování politik za použití jednotlivých opatření, která jsou mapována na interní směrnice nebo externí regulatorní požadavky.
- Nové možnosti reportování souladu podle politik, podle opatření bezpečnosti a podle serverů.
- Proces řízení výjimek pro jejich vytváření a schvalování.
- Schopnost spolupráce při revizi politik a schvalování výjimek s interními i externími auditory.



Uspořádání Opatření



Editor Politik



Zpráva o Shodě

Jak funguje QualysGuard Policy Compliance:

Knihovna Technických Opatření

Knihovna opatření Policy Compliance modulu QualysGuard je založena na zdrojích CIS a NIST. Verze 2.0 podporuje následující oblasti, technologie, standardy a požadavky na soulad:

- **Technologie:** Windows XP Desktop, Windows 2003 Server, Windows 2000 Server, Windows Vista, Windows 2008 Server, RedHat Enterprise Linux 3, 4 a 5, SUSE 9 a 10, Solaris 8, 9, a 10, AIX 5, HPUX 11i.v1, Oracle 9i, 10g a 11g, MS-SQL Server.
- **Standardy a regulatorní požadavky:** CIS, COBIT 4.0 a 4.1, ISO 27001 a ISO 27002, NIST SP800-53, ITIL v2, HIPAA, FFIEC, NERC-CIP, uživatelsky definované odkazy na jednotlivé regulativy.
- **Uživatelsky definovaná opatření:** Možnost návrhu opatření umožní vytvořit technické politiky, které lépe vyhovují požadavkům na shodu a zahrnují hodnoty klíčů v registrech, jejich existence, zápis v ACL a také test existence stávajících a očekávaných souborů na platformě Windows.

Editor Politik

Editor politik QualysGuard je WYSIWYG uživatelské rozhraní umožňující vytvářet a editovat politiky a následně je přiřazovat k jednotlivým aktivům. Politiky mohou být rozděleny do sekcí a mohou obsahovat titulní list pro zaznamenání specifických informací o jejich účelu a způsobu použití v rámci organizace. Uživatel služby má možnost nastavovat očekávané hodnoty, podle kterých se určí, zda je či není stav opatření z dané politiky v souladu.

Výsledky a Výstupy Auditu

Pro práci s výsledky modulu Policy Compliance jsou připraveny nové reporty a workflow pro sledování stavu souladu podle opatření, na jednotlivá aktiva ICT a nebo podle politik. Zahrnuty jsou i volby grafických výstupů pro management organizace. Přizpůsobitelné předlohy reportů o souladu umožňují definovat, které oblasti a informace budou zahrnuty ve výstupní zprávě.

Cena a Dostupnost:

QualysGuard Policy Compliance modul je dostupný jako součást sady QualysGuard Security a Compliance. Cena roční licence QualysGuard Policy Compliance je kalkulována podle počtu IP adres, zahrnuje neomezený počet auditů a 24×7 podporu.

Více informací na http://www.qualys.cz.

Risk Analysis Consultants, s. r.o.
Španělská 2
120 00 Praha 2
Česká republika
telefon: +420 221 628 400
fax: +420 221 628 401
email: qualys@rac.cz
www.rac.cz

Risk Analysis Consultants je nezávislá poradenská společnost poskytující služby a řešení ve všech oblastech bezpečnosti informací v souladu s mezinárodními normami, související národní legislativou a respektováním individuálních podmínek klientů. Od roku 1995 pomáhá zajišťovat bezpečnost informací v informačních systémech organizací státní správy, bank, finančních institucí, telekomunikačních společností a průmyslových podniků v České republice i v zahraničí.

QUALYS®
www.qualys.com

© Qualys, the Qualys logo and QualysGuard are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners. 09/09