

# ServiceNow Security Review

Perché è necessaria una Security Review periodica delle istanze ServiceNow?

La piattaforma **ServiceNow** abilita la digitalizzazione dei processi aziendali e dei flussi di lavoro, in modo estremamente configurabile.

Questa versatilità apre al **rischio di configurazioni errate** e perdita di confidenzialità, integrità o disponibilità delle informazioni gestite.

Studi recenti identificano la **gestione utenti** e le **regole di accesso** quali **aree critiche da attenzionare** ma non sono le uniche. Protiviti propone quindi una security review olistica della piattaforma.



Data-breach dovuti a configurazioni errate\*



Istanze ServiceNow con potenziali data leak\*

(\*): The State of Cloud Security (2021) – Fugue || Major Security Misconfiguration Impacting ServiceNow (2022) – AppOrmi Labs

## Bad-practice nella configurazione delle istanze ServiceNow

- Mancanza di *hardening* di base della piattaforma o difforme dalle linee guida del vendor
- Training non adeguato per lo sviluppo e configurazione sicuri della piattaforma
- Assenza di assessment periodici sulla sicurezza degli sviluppi e delle configurazioni

## ServiceNow Security Review by Protiviti



### Gestione Utenti

- User lifecycle management e utenti guest
- User Authentication & Authorisation
- Configurazione RBAC
- Utenze privilegiate e impersonificazione

### Gestione Procedure e Processi

- Processo di Change Management
- Procedure di Business Continuity

### Gestione Log

- Configurazione di Audit Trail su tabelle
- Log di tracciamento degli accessi
- Analisi periodica o alert di monitoraggio

### Configurazione Piattaforma

- Configurazioni MID Server
- Configurazioni API in e outbound
- Monitoraggio release & patching
- Review ACL e coni di visibilità

### Sicurezza del Codice

- Code Review
- Code Quality Assurance

### Training & formazione

- Configurazione sicura della piattaforma
- Sviluppo sicuro del codice
- Best practice architetturali

Ambiti di analisi

## Vantaggi

- Utilizzo di know-how tecnico in fase di assessment
- Utilizzo di tool già presenti sull'istanza – es. ISC (Instance Security Center)
- Identificazione vulnerabilità e assegnazione rischio pesato in termini sia di business sia di severità tecnica
- Coinvolgimento di tutte le funzioni interessate durante tutto il processo, con limitati impatti
- Coinvolgimento Terze Parti
- Definizione della roadmap per dettagliare il piano tecnico delle bonifiche puntuali
- Supporto continuativo per l'applicazione delle bonifiche suggerite sulla piattaforma

servicenow  
**Partner**  
Elite

Protiviti è **Elite Partner** di ServiceNow ed è in grado di supportare i propri Clienti nell'affrontare gli aspetti di sicurezza dei programmi di trasformazione digitale





# ServiceNow Security Review

Protiviti: Elite Partner ServiceNow

La partnership tra Protiviti e ServiceNow fornisce un approccio innovativo ai nostri servizi di consulenza in materia di **IT Governance, Cyber Security, Governance Risk & Compliance, e Business Process Improvement**, integrando le soluzioni Protiviti con la **tecnologia leader di mercato** di ServiceNow.

<p><b>Dal 2016</b> partner in Italia (6+ anni)</p> 	 <p><b>ELITE Partner in Italia</b></p>	 <p><b>30+</b> <b>Clienti</b></p>	<p><b>35+</b> Risorse con <b>competenze e certificazioni ServiceNow</b> che supportano i Global Service Protiviti</p>  <div style="border: 1px solid white; padding: 5px; display: inline-block;"> <p>ServiceNow <b>Center of Excellence (Italia &amp; Bulgaria)</b></p> </div>
<p>Protiviti ha gestito complessivamente...</p> <div style="text-align: center;">  <p><b>50+</b></p> </div> <p>Progetti ServiceNow</p>			

L'offerta **ServiceNow erogata da Protiviti** è in grado di gestire il processo di adozione della piattaforma ServiceNow end-to-end e di tutti i processi che essa supporta. I nostri servizi sono in genere erogati con un **approccio a fasi** che ne facilita una graduale adozione. Il nostro team può erogare un **mix di servizi su misura per le vostre esigenze**, con un adeguato equilibrio tra **competenze tecniche e di processo**.

 <b>DIAGNOSTICA / ASSESSMENT</b>	 <b>STRATEGIA &amp; ROADMAP</b>	 <b>REQUISITI &amp; PROGETTAZIONE</b>	 <b>SVILUPPO SOLUZIONI</b>	 <b>VALUTAZIONE PERFORMANCE E OPERATIONS</b>
<ul style="list-style-type: none"> <li>• Revisione risk-based di processi, funzioni, tecnologie &amp; metriche</li> <li>• Gap analysis rispetto alle best practice operative e di security</li> <li>• Valutazione della maturità di adozione</li> <li>• Valutazione di aree specifiche per l'efficacia, efficienza, security</li> </ul>	<ul style="list-style-type: none"> <li>• Allineare la visione strategica IT con il modello e gli obiettivi di business</li> <li>• Identificare la sequenza di iniziative da avviare</li> <li>• Identificare i requisiti di risorse e tecnologie</li> <li>• Definire una roadmap strategica per obiettivi</li> </ul>	<ul style="list-style-type: none"> <li>• Prioritizzare le esigenze a breve e lungo termine</li> <li>• Progettare e ingegnerizzare processi e ruoli funzionali</li> <li>• Creare documenti di processo, funzionali e tecnici</li> <li>• Definire requisiti e vincoli delle soluzioni</li> <li>• Assistere nella selezione ed adozione tecnologica</li> </ul>	<ul style="list-style-type: none"> <li>• Configurare e integrare gli strumenti nella soluzione complessiva</li> <li>• Creare funzionalità di reporting e monitoraggio</li> <li>• Testare le soluzioni sviluppate</li> <li>• Gestire le change e i trasporto in produzione</li> <li>• Formare e utenti e amministratori</li> </ul>	<ul style="list-style-type: none"> <li>• Analizzare i dati storici e i report di processo per valutare le capacità di monitoraggio</li> <li>• Identificare le opportunità di miglioramento nei processi esistenti</li> <li>• Definire metriche, KPI e SLA migliorati</li> <li>• Stabilire un processo di monitoraggio continuo</li> </ul>

PROJECT MANAGEMENT, QUALITY ASSURANCE, SECURITY ASSURANCE & REVIEW