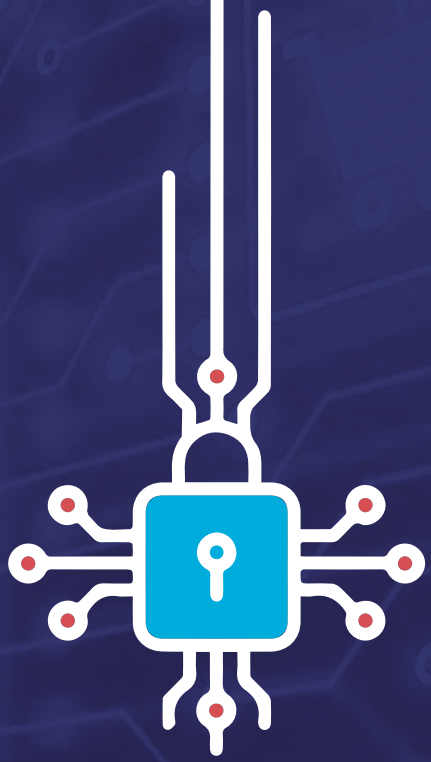
WATI
Delivering Excellence, since 1998



Salesforce's leading SaaS Application Release Management Provider Leverages WATI's

Cybersecurity Services

Problem

The Customer in question was a leader in Application Release Management and 'backup and recovery' for Salesforce. Being a SaaS company, the customer was facing a host of issues in cybersecurity and compliance, upon which the very survival of the company depended. This, in turn, was affecting their relationship with current customers, prospective sales, and deliverability of their services to existing and potential customers, eventually hampering their brand image, reputation and integrity.

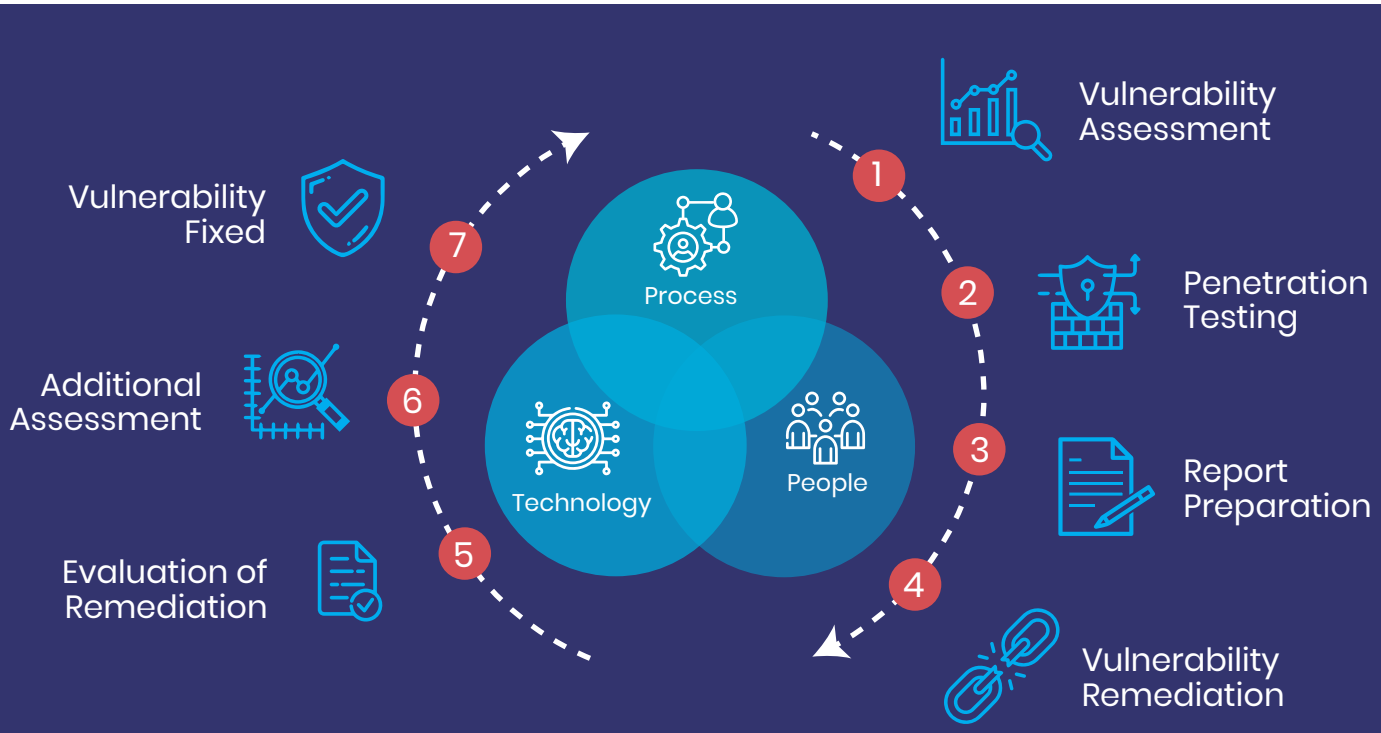
Solution

WATI performed a Comprehensive Penetration Testing – manual, automated and proprietary scripts – against over 66 different types of test cases on the customer's SaaS Applications and IT infrastructure to determine its vulnerability to attacks and the resultant impact of such attacks on the customer's prospective clients. The penetration testing included Network Penetration Testing, Wireless Penetration Testing, SaaS Applications Penetration Testing, and Cloud Infrastructure Penetration Testing.

WATI detailed such vulnerabilities in the form of a Security Audit Report (SAR) and aided the customer in implementing solutions to fix such vulnerabilities and secure it from further attacks in the future. After the customer fixed the vulnerabilities from their end, WATI performed another round of vulnerability assessment and penetration testing to ensure previously identified vulnerabilities were fixed and no additional vulnerabilities crept in.

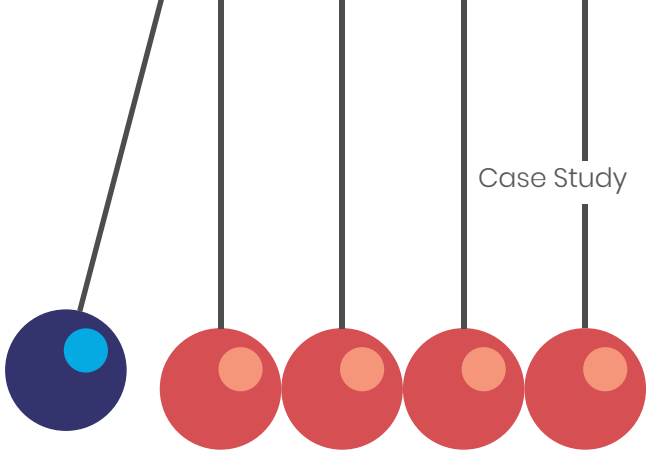
WATI completed penetration testing cycles with great finesse, ensuring no disruption to customer or their clients. WATI followed the recommendations of Open Web Application Security Project (OWASP) and the SANS Institute to test for the top-10 and top-25 vulnerabilities respectively for web applications and infrastructure. The first round of testing resulted in discovery of more than 10 critical vulnerabilities. WATI followed a Common Vulnerability Scoring System, based on which the SAR is generated, which assesses the vulnerability and classifies the risks as 'Critical', 'High', 'Medium', 'Low', and 'Informational'. The SAR includes the vulnerability name, description of such vulnerabilities, details of such vulnerabilities, and solutions to contain or eliminate such vulnerabilities.

Using SAR as a guideline, Customer fixed the vulnerabilities and readied their Applications and infrastructure for 2nd cycle of testing, which happily identified no critical vulnerabilities.



Impact

WATI created a significant impact on its boost their revenues by way of perceived safety in the eyes of the investors and existing and prospective customers. The increasing adoption of SaaS by enterprises also goes in tandem with extra stringent scrutiny for cyber vulnerabilities, so much so that the very survival of SaaS companies and technology vendors solely depend on their perceived safety by enterprises The Customer was perceived as safe, which enabled them to close Series 'A' funding. It also helped them increase their turnaround time of customer deliverability as they could work peacefully without any fear of cybersecurity issues and deliver on their customer promises in time. The Customer also decided to increase the frequency of pentesting cycles to keep up with the release cycles of their products.



Benefits

The reduced number of cyber-attacks, cybersecurity breaches, and cyber risks helped the customer focus on their business without any fear of further cyber-attacks, which positively impacted not only its Return on Investment (RoI), but also its brand image, brand recognition, and brand value, which it was able to sustain for the long-term, thus enhancing their prospective revenues. Moreover, given the effectiveness of the Security Audit, the customer was so delighted with WATI's cybersecurity services that it switched from an Annual cycle which it had initially agreed upon, to a Quarterly cycle.

About WATI

West Advanced Technologies Inc. (WATI), an ISO 27001 company, offers Cybersecurity services including VA/PT, Managed Services, Risk & Compliance Services, Advisory Services, and Training.

SaaS and technology vendors are a focus group for WATI's cybersecurity audits. WATI's Cybersecurity team comprise of experts certified in one or more of CISSP, CISA, CISM, GWAPT, CHFI, CEH, OSCP, CPTE, CWNA, and CompTIA Security+.

Cybersecurity Services	Cyber Risk & Compliance	Cyber Advisory	Cyber Training
Vulnerability Assessment	Seurity Controls	Security Architecture Review	Cybersecurity Bootcamps
Penetration Testing	Gap Assessment	Secure Engineering & Coding	Employee Training
Patch Management	Pre-certification Audit	DevSecOps	Developer Training
Managed Services	Compliance & Certification		Bug-bounty Programs
	Forensic Audit		

Sacramento, CA
Manhattan Beach, CA
Leesburg, VA
Hyderabad , India

Toll-free : +1 (844) 777-WATI (9284)
Phone : +1 (916) 290-6661

Fax : +1 (310) 935-3156
Mail : info@wati.com

www.wati.com