Case Study

Essence of protection

Strengthening network security
with a structured VA/PT program

The Modernization
Engineering Company

SONATA
SONATA SOFTWARE

Summary

Sonata Software partnered with a leading perfume manufacturer to establish a mature, repeatable vulnerability assessment and penetration testing (VA/PT) program. Operating a distributed enterprise network across multiple environments, the client faced configuration drift, residual vulnerabilities, and compliance risks. Sonata implemented a structured VA/PT engagement covering network devices and servers across development, staging, and production environments. This proactive approach delivered a 40% reduction in known vulnerabilities, enhanced audit readiness, and transformed the client's security posture from reactive to proactive—ensuring business resilience and continuous compliance.

Customer overview

A UK-based fragrance manufacturer that has grown into a global leader by focusing exclusively on perfumes, blending creativity with sustainability, and serving some of the world's most recognized brands.

Pressure points

The client operates a distributed enterprise network supporting multiple business-critical applications across development, staging, and production environments. Over time, the network landscape evolved due to infrastructure expansion, technology refreshes, and operational changes, introducing potential security gaps.

Lack of periodic, independent validation of network security controls and configurations.

Residual vulnerabilities persisting due to incomplete remediation or ineffective validation of fixes from previous assessments.

Audit and compliance risk, driven by the absence of a demonstrable, structured vulnerability management lifecycle aligned to industry standards.

Configuration drift across servers and network devices, leading to deviations from CIS hardening benchmarks.

Exposure to emerging threats, where newly discovered vulnerabilities were not being consistently assessed in legacy systems.

Limited internal bandwidth and objectivity, increasing the risk of blind spots when relying solely on internal assessments.

Change-driven risk, as new servers, network devices, and configurations were introduced without standardized security hardening validation.

To address these risks, the client sought to establish a repeatable, structured, and externally validated VA/PT program, conducted once every six months, to strengthen security posture and ensure ongoing compliance.

Solution highlights

Sonata designed and delivered a risk-based, half-yearly VA/PT engagement model, focused on consistency, depth of coverage, and measurable security improvement.

Planning and scope
Established a 6-monthly VA/PT cadence aligned to risk appetite and audit cycles, defined scope across network devices and servers in development, staging, and production environments, aligned assessments to CIS benchmarks and industry best practices, and validated remediation from previous assessments to ensure effective closure.

Periodic vulnerability assessments
Performed end-to-end vulnerability assessments across all in-scope environments to identify missing patches, outdated firmware, weak configurations, insecure services, and exposure to known and emerging vulnerabilities, supported by controlled penetration testing to validate real-world exploitability.

Security posture and trend analysis
Delivered comparative, trend-based insights across assessment cycles to highlight vulnerability recurrence, remediation effectiveness, and systemic weaknesses, enabling data-driven prioritization and continuous security improvement.

Results that speak volumes

Improved security posture
- Achieved a ~40% reduction in known vulnerabilities through structured remediation tracking and validation.
- Reduced the likelihood of exploitable weaknesses remaining undetected between infrastructure changes.

Independent and objective risk visibility
- External assessments provided unbiased validation of internal controls, reducing blind spots.
- Enhanced confidence for senior management, auditors, and stakeholders.

Continuous compliance enablement
- Established a repeatable vulnerability management lifecycle, supporting:
  - Regulatory and customer audit requirements
  - Demonstrable adherence to industry standards
- Simplified evidence generation for audits and certifications.

Proactive risk reduction
- Periodic assessments ensured early identification of emerging threats, minimizing exposure windows.
- Enabled the client to move from a reactive to a proactive security posture.