Case Study

Closing the attack window

Enhancing application security through comprehensive penetration testing

The Modernization Engineering Company

SONATA SOFTWARE

Summary

Sonata partnered with the client to strengthen the security of a business-critical, internet-facing application ecosystem hosted on AWS. Through a comprehensive, risk-driven penetration testing engagement spanning network infrastructure, web applications, APIs, and mobile applications, Sonata simulated real-world adversary techniques to identify exploitable vulnerabilities and end-to-end attack paths. The engagement enabled the client to remediate critical and high-risk security gaps, significantly reducing the likelihood of external exploitation, and improve overall application resilience ahead of regulatory and compliance assessments.

Customer overview

A US-based multinational technology company headquartered in Texas, that designs, develops, and supports a wide range of IT products and services.

Pressure points

The client operated a business-critical, internet-facing application ecosystem hosted on AWS, comprising interconnected network services, web applications, and mobile applications. Given the public exposure and sensitivity of data handled, the client required a deep, attacker-centric security assessment beyond routine vulnerability scanning.

Expanded attack surface due to multiple exposed endpoints across cloud infrastructure, web, and mobile layers

Limited visibility into end-to-end attack paths, particularly across APIs and shared backend services

Business risk exposure, where a breach could result in service disruption, reputational damage, and regulatory penalties

Risk of real-world exploitation, where vulnerabilities across layers could be chained to achieve account compromise or data exfiltration

Regulatory and compliance readiness, requiring independent validation of security controls before formal audits and external reviews

The client's objective was to identify exploitable vulnerabilities and realistic attack paths across all layers of the application stack and remediate critical risks prior to wider exposure and compliance assessments.

Solution highlights

Sonata delivered a comprehensive, risk-driven penetration testing engagement, simulating real-world adversary techniques across network, web, and mobile application layers.

Scoping and test strategy

- Defined a layered penetration testing approach, covering:
  - AWS-hosted network infrastructure
  - Internet-facing web applications and APIs
  - Mobile applications and their backend integrations
- Prioritized assets based on business criticality, exposure, and threat likelihood.
- Aligned testing methodology with industry standards and best practices.

Network penetration testing

- Assessed AWS-hosted network endpoints for:
  - Exposed services and misconfigurations
  - Weak access controls and overly permissive rules
  - Network segmentation and trust boundary weaknesses
- Simulated lateral movement scenarios to identify potential escalation paths within the cloud environment.

Web application penetration testing

- Performed in-depth testing of web applications and APIs, focusing on:
  - Authentication and session management weaknesses
  - Authorization bypass and privilege escalation
  - Input validation flaws and injection risks
  - API security gaps
- Testing aligned with OWASP Top 10 and real-world attack techniques.

Risk-based reporting and validation

- Delivered validated findings with:
  - Clear severity classification
  - Proof-of-concept exploitation evidence
  - Business impact articulation
- Provided practical, prioritized remediation guidance tailored to development and infrastructure teams.

Results that speak volumes

Critical risk reduction

- Identified and enabled remediation of multiple critical and high-risk vulnerabilities across network, web, and mobile layers.
- Significantly reduced the likelihood of successful external exploitation.

Improved attack surface visibility

- Revealed real-world attack paths spanning cloud infrastructure, APIs, web, and mobile applications.
- Enabled the client to understand how seemingly low-risk issues could be chained into high-impact attacks.

Enhanced application resilience

- Strengthened defenses against:
  - Account takeover and credential abuse
  - Sensitive data leakage
  - Unauthorized access to backend systems
- Improved overall robustness of the AWS-hosted application ecosystem.

Actionable security improvements

- Provided clear, prioritized, and implementable remediation guidance.
- Enabled development and infrastructure teams to take immediate corrective action without ambiguity.
- Improved collaboration between security, engineering, and operations teams.