Summary

Sonata conducted a full-scope red team engagement for a multi-property hotel group to simulate real-world cyber-attacks across corporate and property environments. By emulating phishing, external intrusion, and lateral movement scenarios, Sonata helped validate detection and response readiness, uncover credential exposure risks, and strengthen protection of sensitive guest data.

Customer overview

A multi-property hotel group with geographically distributed locations, with a complex IT environment supporting reservation systems, guest services, property management systems, and corporate operations.

Pressure points

Given the hospitality sector's high exposure to cyber threats, the organization sought to validate its real-world resilience against targeted cyber attacks.

- Increased threat targeting of hospitality organizations, including credential theft, ransomware, and data exfiltration.
- High reliance on email and remote access, increasing susceptibility to phishing and social engineering attacks.
- Decentralized property-level environments, creating potential lateral movement paths across hotels.
- Risk to sensitive guest data, including personally identifiable information (PII) and booking details.
- Uncertainty around detection and response effectiveness, particularly during coordinated, multi-stage attacks.
- Need for executive-level assurance, beyond traditional VA/PT, to understand how an attacker could realistically compromise systems.

The objective was to simulate realistic attacker behavior - from initial access through phishing or external intrusion to internal movement - while assessing preventive controls, detection capabilities, and incident response readiness across both corporate and property environments.

Solution highlights

Sonata executed a full-scope red team simulation, combining threat intelligence, social engineering, and technical attack techniques to mirror real-world adversary tactics relevant to the hospitality sector.

Red team planning and scoping
- Designed realistic attack scenarios aligned to hospitality-specific threat models.
  - Covered:
  - External intrusion scenarios
  - Phishing-led initial access
- Internal compromise and lateral movement across hotel properties
- Defined clear rules of engagement to ensure controlled, safe execution.

Threat intelligence–led reconnaissance
- Conducted reconnaissance across:
  - Deep and dark web forums and marketplaces
  - Breach repositories and leak databases
- Identified:
  - Exposed email addresses
  - Potentially compromised credentials
  - Publicly available organizational intelligence
- Used findings to inform phishing and attack simulation scenarios.

Phishing simulation (initial access vector)
- Executed targeted phishing campaigns designed to replicate real-world social engineering attacks.
- Assessed:
  - User susceptibility to phishing
  - Credential exposure risks
  - Effectiveness of email security controls
- Used successful phishing outcomes as a pivot point for further attack simulation.

External attack simulation
- Emulated external threat actors targeting:
  - Internet-facing assets
  - Remote access services
  - Exposed applications and services
- Included credential-based and misconfiguration-driven attack techniques commonly observed in hotel breaches.

Internal compromise and lateral movement
- Simulated post-breach scenarios to evaluate:
  - Privilege escalation opportunities
  - Lateral movement between systems and properties
  - Access to critical business and operational systems
- Assessed segmentation effectiveness between corporate and property networks.

Detection and response evaluation
- Measured:
  - SOC visibility into attacker activities
  - Alerting accuracy and timeliness
  - Incident response coordination and escalation
- Identified gaps in monitoring and response workflows under live attack conditions.

Outcome-driven reporting
- Delivered an executive-level attack narrative, illustrating:
  - End-to-end attack paths
  - Control failures and gaps
  - Supporting evidence and impact analysis
- Provided prioritized, actionable recommendations mapped to people, process, and technology improvements.

Results that speak volumes

Validated real-world security posture
- Demonstrated how a motivated attacker could realistically compromise hotel environments and traverse systems across properties.
- Provided leadership with a clear, practical view of risk exposure.

Confirmed real breach exposure
- Verified the presence and risk of compromised credentials and leaked organizational data.
- Enabled proactive credential resets and control strengthening.

Improved human and technical controls
- Identified gaps in:
  - User awareness and phishing resistance
  - Email security effectiveness
  - Access control and privilege management
- Informed targeted awareness and control enhancement initiatives.

Enhanced detection and response readiness
- Highlighted monitoring blind spots and response gaps against realistic attacker techniques.
- Strengthened SOC readiness through clear improvement actions.

Reduced risk to guest data and hotel operations
- Improved protection of:
  - Booking and reservation systems
  - Guest personal and payment information
  - Property-level operational infrastructure
- Reduced likelihood of service disruption and reputational impact.