

CASE STUDY

Multinational Bank

Comprehensive cyber security assessment for a leading multinational bank with operations across the Middle East, Europe, Asia, and North America

Contents

Overview.....	3
Assessing Cyber Security for Multinational Banking & Financial Services.....	4
Assessment Scope.....	5
1. Vulnerability Assessment and Penetration Testing.....	5
1.1 Core Banking Application Assessment.....	6
1.2 Internet Banking Portal Assessment.....	6
1.3 Mobile Application Security Assessment.....	7
1.4 API Security Assessment.....	7
2. Red Team Assessment.....	8
2.1 Phase 1 – Reconnaissance.....	9
2.2 Phase 2 – Initial Access Campaigns.....	9
2.3 Phase 3 – Lateral Movement and Privilege Escalation.....	9
2.4 Phase 4 – Objective Achievement.....	10
2.5 Purple Team – Collaborative Detection Engineering.....	10
3. Configuration Review.....	11
3.1 Cloud Configuration Review – AWS & Azure.....	11
3.2 Network & Security Device Configuration Review.....	12
3.2 Endpoint Security Review.....	15
4. Security Architecture Review.....	16
Summary of Findings.....	21
Vulnerability Severity Distribution.....	21
Critical Findings.....	22
Remediation and Outcomes.....	23
Regulatory and Standards Alignment.....	24
Why K7 Cyber Security?.....	25

Overview

The Multinational Bank wished to validate the resilience of its technology estate against sophisticated, real-world adversarial threats, in adherence to central bank directives and international regulatory standards. K7 Cyber Security designed and delivered a comprehensive, multi-week cyber security assessment that uncovered critical and high-severity vulnerabilities across the bank's application layer, infrastructure, and operational defences.

2,000+ Identified Areas of Concern	500+ Critical/High Severity Findings	4 Assessment Pillars	15 Countries Covered
--	--	--------------------------------	--------------------------------

Client Snapshot	
Organisation » Headquarters – Middle East » Operational Regions – Middle East, Europe, Asia, North America » Assets Under Management – USD 250+ Billion » Employees – 32,000+	The Multinational Bank operates complex, geographically distributed technology infrastructure that is integral to its core operations, including international and local fund transfers, trade finance, treasury management, and retail mobile banking. The convergence of legacy core banking components with modern API-driven Open Banking services creates a broad and nuanced attack surface requiring deep specialist expertise to analyse. The client benefited from K7's proprietary threat intelligence, deep understanding of banking ecosystem threats, and alignment with frameworks including MITRE ATT&CK, OWASP, CIS Benchmarks, and regional central bank security guidelines.
Technology Landscape » Core Banking Platform – Multi-tenant, hybrid cloud » Mobile Banking – 15+ country-specific applications » Cloud Infrastructure – AWS & Azure (Middle East, Europe, Asia) » Network Estate – 2,000+ devices across branches & data centres » Integration Ecosystem – SWIFT, Open Banking APIs, local payment gateway integrations, SEPA	

Assessing Cyber Security for Multinational Banking & Financial Services

K7's team discussed the bank's IT ecosystem, risk environment, and compliance landscape with the bank's Chief Information Security Officer (CISO), Head of Technology Risk, and regional IT leadership teams, and defined the primary objectives of the engagement:

- **Identify and exploit vulnerabilities** across core banking applications, internet banking portals, and mobile applications deployed in multiple countries
- **Simulate real-world adversarial attacks** including Advanced Persistent Threat (APT) scenarios targeting financial data exfiltration, fraudulent transaction initiation, and privileged access compromise
- **Assess the security posture** of cloud infrastructure (AWS & Azure), network and security devices, and endpoint environments against recognised hardening benchmarks
- **Evaluate the design-level security architecture** of the European regional environments across network, cloud, application, data, and identity/ Zero Trust domains – identifying structural risks that configuration-level reviews alone cannot surface
- **Validate API security controls** across Open Banking interfaces, SWIFT integrations, payment gateway connections, and internal microservices
- **Ensure regulatory alignment** with applicable standards including PCI-DSS, ISO 27001, and relevant regional banking regulations
- **Provide a prioritised remediation roadmap** enabling the bank to systematically address identified risks in alignment with its risk appetite



Assessment Scope

K7 recommended and followed a 4-pillar approach to achieve the identified objectives:

1. VAPT – Core Banking, Internet Banking, Mobile Applications, APIs
2. Red Team Assessment
3. Configuration Review
 1. Cloud
 2. Network & Security Devices
 3. Endpoint Security
4. Security Architecture Review

1. Vulnerability Assessment and Penetration Testing

K7's VAPT engagements are designed to systematically identify and exploit potential vulnerabilities across banking applications, core transaction systems, API endpoints, and third-party integrations. The approach replicates real-world threats targeting payment workflows, SWIFT transfers, fund settlement channels, and customer-facing mobile platforms. K7's security validation covered

- **Authentication and session management** across all customer-facing and back-office interfaces
- **Transaction validation workflows** covering international beneficiary transfers, local beneficiary transfers through regional payment schemes, instant payment networks, and a regional instant payment scheme payment system
- **Backend components** including messaging queues and equation systems underpinning banking transaction processing and message routing
- **Fraud prevention controls** and data privacy mechanisms around critical transaction processing components



1.1 Core Banking Application Assessment

The client's core banking platform – a hybrid multi-tenant environment spanning on-premises and cloud-hosted components – was subjected to comprehensive penetration testing. K7's team assessed

- **Transaction Tampering** – Validation of controls preventing unauthorised modification of transfer amounts, beneficiary details, and value dates during transaction processing
- **Privileged Access Controls** – Assessment of separation of duties, role-based access enforcement, and administrative account security across maker-checker workflows
- **SWIFT Interface Security** – Testing of SWIFT messaging controls, including message authentication, non-repudiation, and resilience against fraudulent payment instruction injection
- **Equation System Integrity** – Review of interest calculation and accounting equation systems for arithmetic manipulation and privilege escalation vulnerabilities
- **Session and API Security** – Validation of session fixation, token replay, and insecure direct object reference vulnerabilities across core banking API layers

Key Finding

K7 identified a critical authentication bypass vulnerability in the back-office transaction authorisation module, enabling a simulated attacker to submit high-value international transfers without secondary approval and bypass the bank's established maker-checker control framework.

This was immediately escalated and remediated.

1.2 Internet Banking Portal Assessment

The bank's internet banking portals – deployed across European and Middle Eastern jurisdictions with separate instances for retail, corporate, and priority banking segments – were assessed using OWASP Top 10 and SANS Top 25 methodologies, supplemented by K7's proprietary financial sector threat intelligence:

- **Cross-Site Scripting (XSS) and CSRF** – Identification and exploitation of stored and reflected XSS vulnerabilities capable of session hijacking and fraudulent transaction initiation
- **Account Enumeration and Brute Force** – Validation of account lockout, CAPTCHA efficacy, and rate limiting across all login and password reset flows
- **Insecure Direct Object References** – Testing of transaction history access controls to prevent unauthorised viewing of other customers' financial data
- **Business Logic Vulnerabilities** – Assessment of transfer limit bypass, duplicate transaction submission, and negative value transfer scenarios
- **SSL/TLS Configuration** – Cipher suite analysis, certificate validation, and HSTS enforcement review across all portal domains

1.3 Mobile Application Security Assessment

Ten country-specific mobile banking applications were assessed across both iOS and Android platforms. Testing was conducted through static analysis, dynamic analysis, and instrumentation-based runtime testing.

- **Insecure Data Storage** – Identification of unencrypted credential storage, sensitive data in device logs, and insecure backup mechanisms
- **Certificate Pinning Bypass** – Assessment of SSL pinning implementation to prevent man-in-the-middle interception of mobile-to-backend API traffic
- **Mobile Wallet Security** – Testing of mobile wallet provisioning, tokenisation controls, and unauthorised transaction initiation from compromised device environments
- **Root/Jailbreak Detection** – Validation of device integrity checks and their bypass potential using commercially available tools
- **API Communication Security** – Testing of all mobile-to-backend API calls for authentication token leakage, parameter tampering, and replay attack vulnerabilities
- **Third-Party SDK Risks** – Review of integrated third-party libraries for known CVEs, excessive permissions, and data exfiltration risks

Key Finding

A high-severity vulnerability was identified in the mobile applications whereby OAuth 2.0 access tokens persisted in plaintext within the application's shared preferences storage – accessible to any application with root-level device access. Immediate patching guidance was provided.

1.4 API Security Assessment

K7 assessed the security of all externally and internally exposed APIs, with particular focus on Open Banking interfaces, payment gateway integrations, and core banking microservices.

- **OAuth 2.0 and Multi-Factor Authentication** – Validation that APIs implement robust authentication and authorisation protocols, ensuring only verified parties can access sensitive customer and transaction data
- **Open Banking API Security** – Assessment of PSD2-compliant Open Banking APIs for authorisation flaws, excessive data exposure, and insecure direct object references
- **Payment Gateway Integrations** – Security testing of local payment gateway integrations, and SEPA payment gateway integrations, including payment redirection tampering, callback manipulation, and HMAC signature validation
- **API Rate Limiting and Throttling** – Validation of controls preventing abusive or automated API consumption targeting account enumeration and transaction flooding
- **GraphQL and REST Endpoint Security** – Testing of introspection exposure, batch query abuse, broken function-level authorisation, and mass assignment vulnerabilities

MITRE ATT&CK Alignment

K7's attack simulations were structured around the MITRE ATT&CK framework, replicating adversarial behaviours documented against the global financial sector. Key simulation scenarios included

- Fraudulent beneficiary addition and transaction tampering via compromised operator sessions
- Unauthorised use of mobile wallets through token replay and device compromise simulation
- API communication manipulation targeting Open Banking data sharing flows
- Reconnaissance, vulnerability scanning, and exploitation chaining to achieve lateral movement from internet-facing components to internal banking infrastructure
- Attempted admin access attainment on key infrastructure components and banking applications through privilege escalation chains

2. Red Team Assessment

K7's Red Team Assessment simulated a full-lifecycle, Advanced Persistent Threat (APT) attack against the bank – replicating the Tactics, Techniques, and Procedures (TTPs) of financially motivated threat actors and nation-state groups historically observed targeting the banking sector.

Only the bank's CISO and a restricted working group were aware of the exercise, enabling K7 to assess the bank's Security Operations Centre (SOC), incident response capability, and human defences without creating artificial bias.



2.1 Phase 1 – Reconnaissance

- **OSINT Collection** – Harvesting of employee credentials from historic breach databases, LinkedIn enumeration of IT and security personnel, and identification of cloud infrastructure through passive DNS and certificate transparency log analysis
- **Attack Surface Mapping** – Enumeration of all internet-facing assets including banking portals, API gateways, VPN endpoints, and cloud management consoles across European and Middle Eastern regions
- **Third-Party Risk Identification** – Mapping of technology vendors, outsourced service providers, and banking technology partners as potential supply chain entry vectors
- **Social Engineering Intelligence** – Collection of organisational hierarchy, IT support procedures, and employee contact data to support targeted phishing campaign design

2.2 Phase 2 – Initial Access Campaigns

- **Spear Phishing** – Targeted email campaigns impersonating internal IT communications, regulatory notices, and vendor correspondence, delivering credential harvesting pages and macro-enabled document payloads to prioritised personnel including Finance, IT, and Operations staff
- **Vishing (Voice Phishing)** – Telephone-based social engineering targeting IT helpdesk and first-line support staff to obtain VPN credentials and reset privileged accounts without proper identity verification
- **External Vulnerability Exploitation** – Exploitation of unpatched vulnerabilities identified on internet-facing systems to establish initial footholds within the bank's DMZ
- **Watering Hole Simulation** – Simulation of third-party vendor portal compromise to assess trust relationships and lateral access potential from supply chain entry points

Key Finding

K7's Red Team successfully obtained valid employee credentials through a targeted spear-phishing campaign within the first 72 hours of the engagement. Critically, no alert was generated by the bank's email security gateway or SOC, demonstrating a significant detection gap in user-targeted attack scenarios.

2.3 Phase 3 – Lateral Movement and Privilege Escalation

- **Credential Harvesting** – Extraction of cached credentials from compromised endpoints using memory forensics techniques, enabling access to additional internal systems
- **Active Directory Exploitation** – Enumeration of Active Directory structure, identification of Kerberoastable service accounts, and execution of pass-the-hash and pass-the-ticket attacks to elevate privileges within the domain

- **Internal Network Pivoting** – Traversal from internet-facing DMZ segments into internal banking network zones, bypassing network segmentation controls through misconfigured firewall rules
- **Cloud Tenant Lateral Movement** – Leveraging compromised on-premises credentials to access cloud management consoles through synchronised identity providers, gaining access to cloud-hosted workloads
- **Persistence Establishment** – Deployment of lightweight persistence mechanisms – scheduled tasks, registry modifications, and rogue service accounts – designed to survive endpoint reboots and credential resets

2.4 Phase 4 – Objective Achievement

Red Team Objective	Achieved	Detected by SOC
Obtain domain administrator privileges	Yes	No
Access core banking administration console	Partial	Partial
Exfiltrate simulated customer PII dataset	Yes	No
Initiate simulated fraudulent payment instruction	Partial	No
Establish persistent access surviving 14 days	Yes	No
Access cloud management console (AWS/Azure)	Yes	No
Compromise SWIFT operator workstation	Partial	Yes

2.5 Purple Team – Collaborative Detection Engineering

K7 also conducted a collaborative Purple Team session with the bank's SOC and Incident Response team. K7's Red Team replayed attack chains in a transparent, controlled manner enabling the bank's defensive team to correlate attacker behaviour with SIEM telemetry, tune detection rules, and build new alerting content mapped to the MITRE ATT&CK techniques demonstrated during the assessment.

Outcomes

- Over two structured Purple Team sessions, the bank's SOC **improved its mean time to detect (MTTD) from an average of 18 hours to under 4 hours** for the specific attack patterns exercised
- **Twenty-three new SIEM detection rules** were authored and validated, directly addressing gaps exposed during the Red Team engagement

3. Configuration Review

3.1 Cloud Configuration Review – AWS & Azure

The bank's cloud estate spans AWS and Azure deployments across data centres in multiple continents, hosting core banking workloads, customer-facing portal infrastructure, data analytics platforms, and DevOps toolchains. K7 assessed the following control domains:

Identity and Access Management (IAM)

- Enumeration and assessment of all IAM roles, policies, and permission boundaries across AWS accounts and Azure subscriptions
- Identification of overly permissive IAM policies granting wildcard resource access – a persistent risk enabling lateral movement within cloud tenants
- Validation of multi-factor authentication enforcement for all privileged IAM users, service accounts, and federated identity providers
- Review of cross-account role trust relationships and external identity provider configurations for unauthorised delegation

Storage and Data Security

- Assessment of S3 bucket and Azure Blob storage access policies – identifying publicly accessible storage resources containing sensitive banking configuration and application data
- Validation of encryption-at-rest enforcement (AES-256/AWS KMS/Azure Key Vault) for all storage resources containing customer and transaction data
- Review of data lifecycle policies, retention controls, and cross-region replication security for regulatory compliance

Network Security Controls

- Review of Security Group and Network Security Group (NSG) configurations – identifying unnecessarily permissive inbound rules exposing management ports (SSH, RDP, WinRM) to wide internet ranges
- Assessment of VPC/VNet peering configurations, transit gateway routing, and network segmentation between production, development, and management environments
- Validation of Web Application Firewall (WAF) rule sets protecting externally exposed application load balancers and API gateways

Logging, Monitoring, and Incident Response

- Assessment of AWS CloudTrail, AWS Config, Azure Monitor, and Microsoft Defender for Cloud coverage and retention configuration
- Identification of gaps in logging coverage across critical services including EC2, Lambda, RDS, and Azure SQL Database
- Review of GuardDuty and Microsoft Sentinel alerting rules against known cloud-specific attack patterns

Key Finding

K7 identified 11 S3 buckets and 4 Azure Blob storage containers with misconfigured public access permissions, collectively exposing application configuration files, internal API documentation, and historical transaction log extracts. Additionally, three AWS IAM roles carried wildcard action policies effectively granting full-account administrative access to associated workloads.

3.2 Network & Security Device Configuration Review

K7 reviewed the configuration of more than 1,800 network and security devices across the bank's headquarters, data centres, and branch offices in multiple countries. The assessment covered the full breadth of the infrastructure stack – perimeter and internal networking, security gateways, storage and database platforms, monitoring and detection infrastructure, and availability protection systems.

All devices were benchmarked against CIS Benchmarks, vendor hardening guides, and the bank's internal baseline standards.

Firewall Policy Review

- Assessment of perimeter and internal firewall rule sets for overly permissive access rules, shadowed rules, and rule base bloat accumulated over time
- Identification of any-to-any rules in production firewall policies – particularly between PCI-scoped network segments and adjacent corporate zones
- Validation of outbound traffic filtering controls preventing data exfiltration via unusual protocols and ports

Switch and Router Hardening

- Review of device management access configurations – Telnet usage, unencrypted SNMP community strings, and default credential retention
- Assessment of spanning tree protection (BPDU guard, root guard), DHCP snooping, and dynamic ARP inspection configurations
- Validation of routing protocol authentication (OSPF, BGP MD5/SHA) and route filtering controls

Network Segmentation

- Assessment of VLAN design and inter-VLAN routing controls segregating PCI cardholder data environments from corporate networks
- Validation of network micro-segmentation controls within cloud-adjacent data centre environments
- Review of out-of-band management network isolation from production traffic paths

Email Security Gateway

- Review of inbound mail filtering policies – SPF, DKIM, and DMARC enforcement, sender reputation thresholds, and quarantine workflow effectiveness
- Assessment of attachment sandboxing, URL rewriting, and click-time protection controls against credential-phishing and malware-delivery campaigns
- Validation of outbound Data Loss Prevention (DLP) rules covering customer PII, payment card data, and confidential banking communications
- Review of administrative access controls, role separation, audit logging, and integration with the SIEM for phishing and BEC alert correlation

SAN Storage Infrastructure

- Assessment of SAN fabric zoning configuration – single-initiator zoning enforcement, removal of stale or orphaned zones, and prevention of cross-tenant LUN exposure
- Validation of storage controller management plane security – administrative access hardening, encrypted management protocols (HTTPS/SSH only), and elimination of default service accounts
- Review of data-at-rest encryption coverage across LUNs hosting core banking, SWIFT, and customer data repositories, including key management lifecycle controls
- Assessment of snapshot, replication, and backup target configurations to ensure ransomware resilience and integrity of recovery copies

Database Platforms

- CIS Benchmark assessment of Oracle, Microsoft SQL Server, and PostgreSQL instances hosting core banking, transaction, and customer data stores
- Review of privileged database accounts (SYSDBA, sa, superuser), password vaulting, dormant account detection, and separation of duties between DBAs and application owners
- Validation of Transparent Data Encryption (TDE), column-level encryption for sensitive fields, and TLS enforcement on all database listener endpoints
- Assessment of database audit logging coverage, log forwarding to the SIEM, and detection rules for sensitive data access, schema changes, and bulk export activity
- Review of patch currency across database engines and the underlying operating system, with identification of unpatched CVEs in production environments

SIEM Platform

- Review of log source coverage – completeness of ingestion from firewalls, endpoints, EDR, cloud control planes, identity providers, core banking applications, and database audit streams
- Assessment of detection rule library against the MITRE ATT&CK framework, with gap analysis covering banking sector TTPs (BEC, SWIFT-targeted attacks, payment fraud, insider misuse)
- Validation of correlation logic, alert deduplication, suppression rules, and tuning of false-positive-prone signatures
- Review of SIEM platform hardening – administrative access controls, role-based access for analysts, integrity of stored log data, and retention alignment with regulatory requirements
- Assessment of integration with the SOAR layer for automated triage, enrichment, and containment playbook execution

DDoS Protection

- Review of volumetric and protocol-layer DDoS mitigation coverage across internet-facing banking portals, API gateways, and Open Banking endpoints
- Assessment of application-layer (Layer 7) protection profiles – rate limiting, JavaScript challenges, CAPTCHA fallback, and bot management against credential-stuffing and account-takeover campaigns
- Validation of always-on versus on-demand mitigation posture, BGP/DNS redirection readiness, and time-to-mitigate metrics against documented service-level objectives
- Review of upstream provider scrubbing capacity, failover paths, and tested runbooks for sustained large-scale attack scenarios

Load Balancers & Application Delivery Controllers

- Assessment of SSL/TLS termination configuration – cipher suite selection, certificate validity and rotation, OCSP stapling, and HSTS enforcement on customer-facing virtual servers
- Review of management plane hardening, administrative authentication (RADIUS/TACACS+ integration), and elimination of default credentials and unused service accounts
- Validation of application-layer security policies – request inspection rules, header sanitisation, and integration with upstream Web Application Firewall enforcement
- Review of high-availability and session persistence configurations to ensure resilience without weakening application security controls

Key Findings

K7 identified 18 firewall rules permitting broad any-to-any traffic between corporate office segments and internal data centre zones – effectively negating segmentation controls. SNMP v1/v2c with default community strings was confirmed active on 47 network devices. The email security gateway was running with DMARC enforcement set to 'none' on the primary banking domain, allowing direct-spoof phishing into staff mailboxes. SAN fabric zoning was found to be overly broad in two data centres, with management database accounts using shared service credentials across production and non-production environments. The SIEM platform had material log-source gaps for two cloud workload categories, and DDoS protection on three customer-facing portals operated in on-demand mode with no documented activation runbook.

3.2 Endpoint Security Review

Endpoints across the bank's estate – including servers, corporate workstations, and privileged administrative jump hosts – were assessed for compliance with established hardening baselines and endpoint security control effectiveness:

- **Operating System Hardening** – CIS Benchmark compliance assessment across Windows Server, Windows 10/11, and Linux endpoints – covering account policy, auditing, service configuration, and registry hardening
- **Patch Management Posture** – Assessment of patch currency across all endpoint categories, with identification of critical and high-severity unpatched CVEs across Windows, Linux, and third-party application components
- **EDR Coverage and Configuration** – Validation of Endpoint Detection and Response (EDR) agent deployment coverage, policy configuration, and integration with the bank's central SIEM platform
- **Privileged Access Management** – Assessment of local administrator account management, privileged account usage patterns, and credential hygiene across all endpoint categories
- **Application Allowlisting** – Review of application control policy effectiveness and identification of policy bypass vectors using living-off-the-land binaries (LOLBins)

4. Security Architecture Review

K7 conducted a multi-domain Security Architecture Review of the bank's regional environments in 2 European countries that were selected as the focus geographies because they host the largest concentration of European retail, corporate, and Open Banking workloads, fall under particularly prescriptive regulatory regimes, and were the original deployment templates for the bank's broader EU rollout.

The review was scoped across five interlocking domains – network architecture, cloud architecture, application architecture, data and database architecture, and identity and Zero Trust architecture – and benchmarked against the NIST Cybersecurity Framework, SABSA, CIS Critical Security Controls v8, and the bank's own target reference architecture.



Network Architecture

K7 reviewed the regional network architecture across both data centres and branch estates in the European countries, focusing on zone design, segmentation strategy, north-south and east-west traffic controls, and resilience of the regional internet edges:

- **Zone Topology & Segmentation** – Review of the bank's security zone model (untrusted, DMZ, application, data, management, OOB) and the consistency of its implementation across the data centres – including evaluation of inter-zone firewall enforcement points and shared-services trust assumptions
- **East-West Traffic Control** – Assessment of intra-data-centre segmentation between core banking, customer-facing, analytics, and corporate-IT workload tiers, including the role of internal firewalls, micro-segmentation, and software-defined controls
- **Regional Internet Edges & Interconnects** – Review of internet ingress/egress architecture – load balancer placement, WAF and DDoS scrubbing positioning, and the design of inter-region connectivity (MPLS, SD-WAN overlays, cloud on-ramps) between the European centres and the wider group network
- **Branch Network Design** – Evaluation of branch-to-data-centre connectivity, the security stack deployed at branches, and the trust posture assumed for branch-originated traffic accessing core banking services
- **Out-of-Band Management Architecture** – Validation of dedicated management network design separating administrative access paths from production data traffic, including jump host architecture and privileged session brokering

Cloud Architecture — AWS & Azure

The bank's cloud architecture in Europe was reviewed across both AWS and Azure footprints, with particular attention to landing-zone design, workload placement, and the security control plane:

- **Landing Zone & Account Strategy** – Review of AWS Organisations/Azure Management Group hierarchy, account/subscription separation by environment and workload, and consistency of guardrails (SCPs, Azure Policy) enforced at the landing-zone level across the European facilities
- **Network Architecture in Cloud** – Evaluation of VPC/VNet design, hub-and-spoke topology, transit gateway and virtual WAN routing, and the placement of inspection points (firewalls, NVAs, native security services) for north-south and east-west traffic
- **Workload Placement & Data Residency** – Assessment of how workloads are mapped to the European cloud regions in alignment with data residency expectations – and the controls preventing accidental cross-border data movement
- **Cloud-to-On-Premises Connectivity** – Review of Direct Connect/ExpressRoute architecture, BGP design, redundancy, and the security controls applied to traffic transiting the cloud-on-premises boundary
- **Cloud-Native Security Control Plane** – Evaluation of the architectural role of AWS Security Hub, GuardDuty, Microsoft Defender for Cloud, and Sentinel – including telemetry aggregation patterns, multi-account/multi-subscription coverage, and integration with the central SOC

Application Architecture

Application architecture was reviewed for the customer-facing and internal banking platforms deployed across the European stacks, with focus on security boundaries, integration patterns, and the placement of security controls within the application fabric:

- **Tiering & Component Boundaries** – Review of presentation, application, integration, and data-tier separation across internet banking, mobile backend, and Open Banking services – including evaluation of trust assumptions between tiers and the controls enforcing them
- **API Gateway & Service Mesh Design** – Assessment of API gateway placement, authentication and authorisation enforcement, rate limiting and quota architecture, and the role of any service mesh in east-west service-to-service security
- **Open Banking Architecture** – Review of the PSD2 Open Banking architecture in the European facilities – including consent management flows, TPP onboarding, and the segregation of Open Banking exposure from core banking systems
- **Secure SDLC & DevSecOps Architecture** – Evaluation of the CI/CD architecture supporting the European deployments – branch protection, artifact integrity, secrets management, and the placement of SAST, SCA, DAST, and IaC scanning gates in the pipeline
- **Resilience & Failure Domain Design** – Review of application failure domain isolation, blast-radius containment, and the architectural treatment of dependencies on shared regional services (DNS, certificate authorities, secret stores)

Data & Database Architecture

The data architecture review examined how customer, transaction, and operational data is stored, classified, replicated, and protected across the European environments – and how that design supports regulatory obligations.

- **Data Classification & Flow Architecture** – Review of the bank's data classification model, mapping of regulated data domains (PII, payment card data, PSD2 account data) to underlying data stores, and architectural visibility of data flows across the European environments
- **Database Topology & Tenancy** – Assessment of the topology of core banking, payments, customer, and analytics databases – instance separation, multi-tenancy boundaries, and the segregation of production data from non-production environments
- **Encryption Architecture** – Evaluation of encryption-at-rest and in-transit design across the data estate, including key management architecture (HSM, KMS, Azure Key Vault), key lifecycle ownership, and the separation of key custodianship from data custodianship
- **Backup, Replication & Recovery Architecture** – Review of cross-site and cross-region backup architecture, immutability controls against ransomware, and the security architecture of the recovery path itself (restoration credentials, network isolation of recovery environments)
- **Data Loss Prevention & Tokenisation Architecture** – Assessment of the architectural placement of DLP enforcement, tokenisation vaults for payment card data, and data masking patterns supporting development and analytics consumption
- **Cross-Border Data Movement** – Review of architectural controls preventing unintended movement of European regulated data into other group regions



Identity & Zero Trust Architecture

K7 reviewed the identity and Zero Trust architecture supporting European operations, evaluating both human and non-human identity treatment:

- **Identity Provider Architecture** – Review of the primary identity provider topology (Azure AD/Entra ID, on-premises Active Directory, federated providers), the trust relationships between them, and the consistency of the identity fabric across the European facilities
- **Authentication Architecture** – Evaluation of authentication patterns – MFA enforcement points, phishing-resistant authenticator coverage for privileged users, conditional access design, and the architectural treatment of legacy authentication protocols
- **Authorisation & Access Model** – Review of the role-based and attribute-based access architecture across core banking, cloud, and SaaS estates, including just-in-time elevation patterns and the architectural separation between standing and privileged access
- **Privileged Access Architecture** – Assessment of the privileged access management (PAM) architecture – vault placement, session brokering design, tier-0 isolation patterns, and the secure administrative workstation model used by European privileged operators
- **Non-Human Identity Architecture** – Review of service account, workload identity, and machine-to-machine credential architecture, including the use of managed identities, workload federation, and the lifecycle of long-lived secrets in pipelines and applications
- **Zero Trust Maturity Assessment** – Evaluation of European facility environments against a Zero Trust maturity model – identity-centric controls, device trust, network as untrusted, application-aware policy enforcement, and continuous verification posture

Key Findings

K7 discovered that the European environments shared a flat tier-0 trust boundary – privileged identities created in one region carried implicit administrative trust into the other through synchronised identity providers, with no architectural enforcement of regional isolation at the privileged-access layer. In parallel, the Open Banking exposure in both regions was deployed on shared application infrastructure with the internet banking stack, providing no architectural blast-radius containment between PSD2-exposed services and customer-authenticated banking services. Both findings were classed as design-level risks requiring strategic remediation rather than configuration fixes.

Cross-Regional Architecture Comparison

A specific deliverable of the engagement was a comparative view of European facility architectures, highlighting where the two regions diverge unintentionally and where one region's stronger design could be promoted as the group standard.

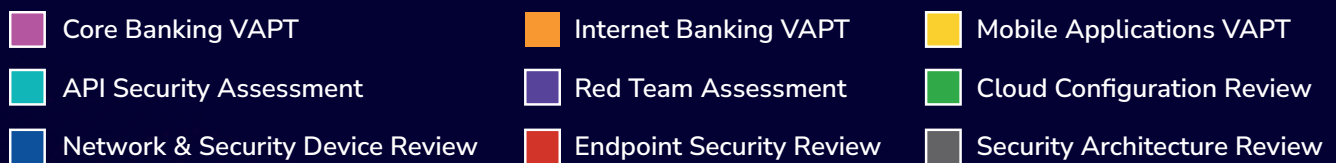
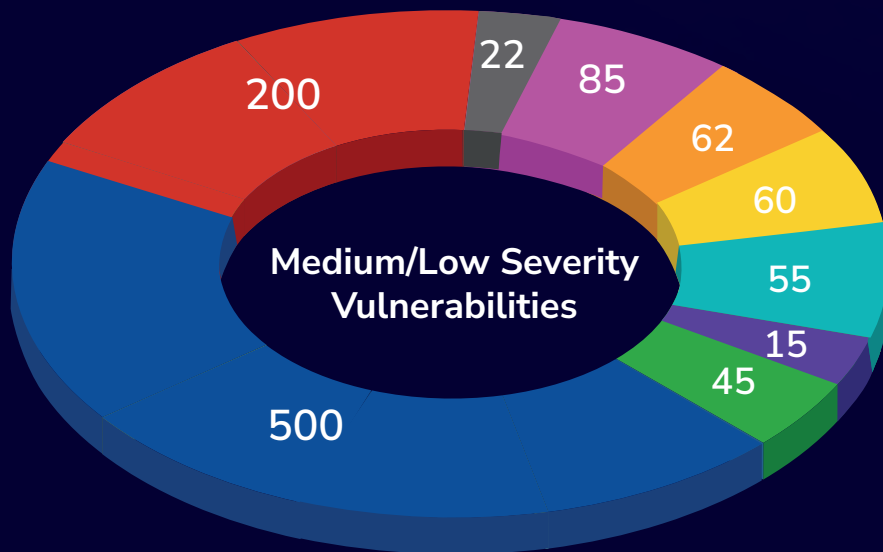
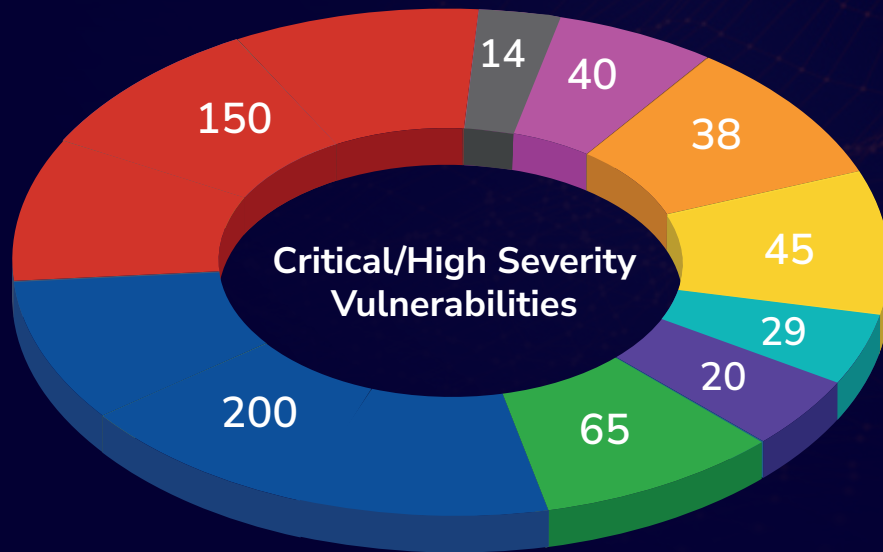
Architecture Domain	Region 1	Region 2
Network Segmentation Maturity	Established	Established
Cloud Landing Zone Guardrails	Partial	Established
Open Banking Isolation	Shared Stack	Shared Stack
Privileged Access (Tier-0 Isolation)	Cross-Trusted	Cross-Trusted
Encryption Key Custodianship	Centralised	Regional
Zero Trust Maturity	Developing	Developing
Data Residency Enforcement	Established	Established

Outcome

K7 delivered a target-state architecture roadmap covering all five domains, prioritised across a 12-month horizon. Specific structural recommendations included the introduction of regional tier-0 isolation between European privileged identity planes, architectural separation of Open Banking exposure onto a dedicated landing zone, harmonisation of cloud landing-zone guardrails using a facility's stronger baseline as the group standard, and a Zero Trust maturity uplift programme anchored on identity-centric policy enforcement.

Summary of Findings

Vulnerability Severity Distribution



Critical Findings

Finding	CVSS Score
Domain Compromise via Red Team – Full Active Directory domain administrator compromise achieved within 5 days of initial phishing access	10.0
Core Banking Auth Bypass – Authentication bypass in transaction authorisation module enabling maker-checker control circumvention	9.8
Cross-Region Tier-0 Trust (Architecture) – Privileged identities in the European facilities share an implicit administrative trust boundary through synchronised IdPs, with no architectural enforcement of regional isolation	9.1
Open Banking Shared-Stack Exposure (Architecture) – Open Banking (PSD2) services deployed on shared application infrastructure with internet banking, providing no architectural blast-radius containment	8.9
Mobile Token Plaintext Storage – OAuth 2.0 access tokens stored in plaintext shared preferences across mobile applications in the Middle East	8.8
S3 Bucket Public Exposure – 11 S3 buckets with public read access exposing internal configuration, API documentation, and transaction log data	8.5
Firewall Any-to-Any Rules – Broad any-to-any firewall rules between corporate and data centre zones effectively eliminating network segmentation controls	8.1
Email Gateway DMARC Misconfiguration – Primary banking domain operating with DMARC policy set to 'none,' enabling direct-spoof phishing campaigns against staff and customers	8.1
SIEM Log Source Gaps – Material logging gaps across two cloud workload categories, reducing detection visibility for cloud-native attack patterns	8.0
SWIFT Workstation Hardening Gap – Insufficient endpoint hardening and monitoring on SWIFT operator workstations enabling lateral movement simulation	8.0

Remediation and Outcomes

K7's engagement extended beyond identification of vulnerabilities to active remediation guidance and post-fix validation. A structured remediation programme was delivered in four phases.

Phase	Timeline	Remediation
1 – Immediate Actions	0-30 Days	• Critical and High-severity Findings ◦ Patch deployment ◦ Firewall rule remediation ◦ IAM policy correction ◦ Mobile application updates ◦ DMARC enforcement on the primary banking domain ◦ S3 bucket access revocation
2 – Strategic Hardening	30-90 Days	• Medium-severity remediation • Network segmentation redesign • Cloud Security Posture Management (CSPM) tooling deployment • SIEM log-source completeness programme • SAN zoning remediation • Privileged access management programme enhancement
3 – Architectural Uplift	90-180 Days	• Implementation of the target-state architecture roadmap from the Architecture Review ◦ Regional tier-0 isolation between European privileged identity planes ◦ Separation of Open Banking exposure onto a dedicated landing zone ◦ Harmonisation of cloud landing-zone guardrails using the facility with the stronger baseline as the standard ◦ Phase 1 of the Zero Trust maturity uplift
4 – Continuous Improvement	180+ Days	• Establishment of a quarterly VAPT cycle • Integration of K7's threat intelligence feeds into the bank's SIEM • SOC training programme based on Red Team findings • Annual Red Team and Architecture Review scheduling

Remediation Outcomes

- Within 45 days of final report delivery, the bank successfully remediated 100% of Critical-severity findings and 87% of High-severity findings
- K7 conducted formal re-testing of all Critical- and High-severity findings, issuing a Remediation Validation Certificate confirming effective closure
- Architectural recommendations were accepted into the bank's strategic technology roadmap, with the tier-0 regional isolation and Open Banking landing-zone separation entering design execution within the 90-day window
- The bank's overall security posture score – assessed against K7's proprietary banking sector maturity model – **improved from 42% to 71%** following remediation

Regulatory and Standards Alignment

All K7 assessment activities were conducted in alignment with applicable regulatory frameworks and international standards.

Framework/Standard	Application
MITRE ATT&CK Framework	Structuring of Red Team TTPs and detection engineering outcomes
OWASP Top 10/ASVS	Web and API vulnerability classification and testing guidance
CIS Controls & Benchmarks	Configuration hardening baselines for cloud, network, security devices, and endpoint assets
NIST Cybersecurity Framework	Structuring of the Architecture Review across Identify, Protect, Detect, Respond, and Recover functions
SABSA	Business-driven security architecture methodology applied to the multi-domain Architecture Review
PCI-DSS v4.0	Payment card industry data security requirements applied to cardholder data environments
ISO/IEC 27001:2022	Information security management system requirements informing control assessment scope
NIST SP 800-53 Rev 5	Security and privacy controls framework applied to cloud workload assessments

In addition, relevant regional banking regulations were considered and adherence to stipulated cyber security standards was verified during the engagement.

Why K7 Cyber Security?

K7 Cyber Security brings over three decades of deep cyber security expertise to every engagement. Our competitive differentiation in banking and financial services security assessments is grounded in:

Proprietary Threat Intelligence	Proprietary AV & Detection Engine
K7's in-house threat research team continuously analyses the global threat landscape, with specific focus on banking-sector malware, APT campaigns, and financial fraud methodologies – ensuring assessments reflect the threats your organisation actually faces.	Unlike system integrators repackaging third-party tools, K7 develops and maintains its own anti-malware detection engine – providing deeper insight into malware behaviour observed during assessments and enabling more accurate risk quantification.
Deep Banking Sector Expertise	Multi-Regional Regulatory Knowledge
Our specialists understand core banking architectures, SWIFT ecosystems, Open Banking regulatory requirements, and regional payment schemes – enabling assessment that is both technically rigorous and contextually relevant.	K7 maintains active knowledge of regulatory requirements across our four operational geographies – India, Singapore, UAE, and the USA – and extends this to European regulatory contexts, ensuring all engagements are compliance-relevant.
GRC & Compliance Leadership	Proprietary SIEM & Enterprise SOC Operations
K7's GRC practice is led by certified Lead Implementers and Lead Auditors across ISO 27001, ISO 27701, ISO 42001, PCI-DSS, GDPR, DPDP, NESA, and UAE IA – practitioners with genuine management consulting depth, not just checklist familiarity. During security assessments, this translates directly into richer findings: our consultants contextualise technical vulnerabilities within your regulatory obligations, governance gaps, and board-level risk appetite, ensuring that every remediation recommendation is compliance-ready and carries measurable business value for your bank.	K7 has built and operates its own SIEM platform, running 24/7 SOC services for enterprise clients across multiple industries. Our Blue Team and Red Team analysts are updated weekly with intelligence from K7 Labs' malware reverse engineering team – meaning our assessors can examine a threat at binary and code level, not just through a generic tool's alert. This 33-year cyber security DNA, embedded into every engagement, ensures your bank receives an assessment grounded in live adversarial reality, delivering genuine return on investment on your security spend.



Copyright © 2026 K7 Enterprise Security Private Limited, All Rights Reserved.

This work may not be sold, transferred, adapted, abridged, copied, or reproduced in whole or in part in any manner or form or any media without the express prior written consent of authorised personnel of K7 Enterprise Security Private Limited. All product names and company names and logos mentioned herein are the trademarks or registered trademarks of their respective owners.

www.k7cybersecurity.com