SIDEKICK SECURITY

CASE STUDY

Full-Spectrum Security Improvements for the Credit Union Sector

2025 – 2026

EXECUTIVE SUMMARY

> *Across seven distinct security domains — physical intrusion, internal and external network penetration testing, cloud security, web application assessment, SaaS configuration review, phishing resilience evaluation, and infrastructure threat modeling — Sidekick Security demonstrated that even mature organizations carry compounding vulnerabilities that only a full-spectrum assessment methodology can reveal.*

Between late 2025 and early 2026, Sidekick Security conducted a comprehensive series of security assessments spanning the physical, network, cloud, application, and organizational security domains. This case study covers work that our team did with four different credit union organizations across 18 locations in multiple states, demonstrating Sidekick's full-spectrum capabilities in areas directly applicable to financial services operational environments.

The combined body of work reveals a consistent theme: organizations that invest in point-solution security controls such as badge readers, firewalls, and endpoint protection remain exposed when those controls are not validated under realistic adversarial conditions. Sidekick's methodology bridges this gap by testing across every domain an attacker would exploit, chaining findings into compound attack scenarios, and delivering deployable remediations that close gaps immediately.

This case study documents the breadth and depth of Sidekick's security assessment capabilities, the cross-domain vulnerability chains that emerge when organizations are assessed holistically, and the unique post-engagement partnership model that accelerates remediation and program maturity.

4+	18	7	50+	6
ORGANIZATIONS	LOCATIONS	DOMAINS TESTED	CRITICAL FINDINGS	REAL-WORLD ATTACK CHAINS

CLIENT PROFILE

Industry	Financial Services — Credit Unions & Shared Service Providers
Organization Scope	Corporate offices, branch locations, shared service centers, cloud infrastructure, and SaaS platforms
Geographic Footprint	Maryland (Baltimore metro) and Colorado (Denver metro)

Regulatory Environment	NCUA Part 748, GLBA Safeguards Rule, PCI-DSS, FFIEC, SOC 2, NIST CSF
Assessment In-Scope Domains	Physical facilities, wireless, internal/external network, cloud (Azure), web application, SaaS, phishing resilience, and threat modeling
Engagement Duration	Multiple engagements spanning October 2025 – January 2026

THE CHALLENGE

Credit unions face a threat landscape that extends far beyond physical premises or corporate IT. As member-owned financial institutions, they are custodians of sensitive personal and financial data while operating under strict federal regulatory oversight. Many organizations have invested in cybersecurity controls and tools, yet the interconnections between physical security, network infrastructure, cloud environments, SaaS platforms, and human factors create compound attack surfaces that point-solution testing and remediation support cannot reveal.

Modern credit union infrastructure typically spans a mix of on-premises networks with Active Directory, Azure cloud services, member-facing web or mobile applications, dozens of SaaS platforms supporting operations and member services, and distributed branch locations; each representing a distinct attack vector that adversaries can chain together. Board-level pressure, evolving NCUA examination expectations, and an escalating threat environment demanded a comprehensive assessment approach that mirrors how real attackers operate: across every domain, simultaneously.

Key Concerns

- Physical access controls, employee awareness, and visitor management procedures untested under realistic adversarial conditions across corporate and branch environments
- Internal network architectures unvalidated against modern attack techniques including Active Directory exploitation, Kerberoasting, and lateral movement
- Cloud infrastructure (Azure) security posture unassessed for misconfigurations in identity, encryption, network controls, and key management
- Web applications handling sensitive member data untested for authorization flaws, injection vulnerabilities, and cache poisoning attacks
- SaaS platform sprawl creating shadow IT risks with ungoverned access, privilege escalation, and data exposure
- Phishing resilience unmeasured, with reliance on push-notification MFA instead of phishing-resistant FIDO2 authentication
- No comprehensive threat model documenting how threat actors could chain vulnerabilities across hybrid on-premises and cloud environments

THE APPROACH

Sidekick Security designed a full-spectrum assessment program covering every domain a sophisticated adversary would target. Each engagement was tailored to the organization's specific environment, rooted in a threat profile with tailored capabilities, while applying a consistent methodology that maps findings across domains, identifies compound attack chains, and delivers deployable remediations, not just a report of vulnerabilities.

The approach combined hands-on adversarial testing with structural configuration reviews and strategic threat modeling, ensuring that both exploitable vulnerabilities and architectural weaknesses were identified and contextualized within the credit union regulatory environment.

Services Delivered

SERVICE	DESCRIPTION
Physical Penetration Testing	Multi-day physical intrusion testing across corporate offices, branches, and data centers using realistic pretexts including contractor impersonation, interview scenarios, and badge fabrication
Wireless Security Assessment	Comprehensive wireless reconnaissance, WPA3-SAE evaluation, rogue AP detection, segmentation validation, and cross-environment baseline analysis
Internal Network Penetration Testing	Full-scope Active Directory testing including password spraying, Kerberoasting, NTLM relay, Shadow Credentials exploitation, and domain compromise path analysis via BloodHound
External Network Penetration Testing	OSINT-driven reconnaissance, email security validation (DMARC/SPF/DKIM), service account enumeration, MFA bypass testing, and external attack surface mapping
Cloud Security Assessment (Azure)	Azure subscription review covering identity and access management, Key Vault security, network controls, encryption configuration, activity log monitoring, and compliance mapping
Web Application Penetration Testing	Authorization testing (IDOR), injection analysis, cache poisoning, security header evaluation, and session management review for member-facing applications
SaaS Configuration Review	Platform security assessment covering access controls, privilege escalation paths, data sharing policies, audit logging, and shadow IT governance across M365 and operational SaaS tools
Phishing Resilience Assessment	Email security posture evaluation (DMARC/SPF/DKIM), MFA strength analysis, browser security controls, security awareness baseline, and incident response readiness
IT Infrastructure Threat Modeling	Strategic threat analysis across hybrid cloud infrastructure identifying threat actors, attack scenarios, critical asset exposure, and prioritized risk mitigation roadmap

KEY FINDINGS

Across all assessment domains, Sidekick Security identified over 50 findings spanning physical access control failures, Active Directory misconfigurations, cloud security gaps, web application authorization flaws, SaaS governance weaknesses, phishing susceptibility, and architectural risks. That said, the number of findings is a vanity metric that doesn't actually move the needle or translate to real organizational risk.

The findings below highlight the most impactful vulnerabilities from each domain, each representative of systemic challenges facing credit unions and financial institutions industry-wide.

Physical & Social Engineering

HIGH

Unauthorized Physical Access via Tailgating and Social Engineering — 100% Success Rate

Assessors successfully bypassed access-controlled entry points at every organization tested. Techniques included piggybacking through turnstiles, tailgating through badge-reader doors, and following employees through secured entrances without challenge. In multiple cases, assessors moved freely through restricted office spaces for 20+ minutes without intervention, accessing server rooms, electrical panels, and areas containing member data.

HIGH

Exposure of Critical Infrastructure — Server Rooms, Electrical, & Fire Systems

At three of four organizations, assessors gained unescorted access to server rooms, electrical distribution panels, fire alarm control units, and telecommunications infrastructure. Staff accepted contractor pretexts at face value, provided access to locked areas, and returned to their desks, leaving assessors unsupervised with critical systems that facilitated access to corporate or internal network resources.

Network

CRITICAL

Full Active Directory Domain Compromise via Attack Chain

Starting from unauthenticated network positions, the assessment team achieved full Domain Administrator access through a multi-step attack chain: null session enumeration of domain controllers revealed user accounts, password spraying identified accounts using weak credentials, Kerberoasting extracted crackable service account hashes, and a Shadow Credentials attack against a privileged service account completed the compromise. The entire chain, from basic network access to Domain Admin, was typically executed within a single business day.

HIGH

Sensitive Documents Stored Insecurely on Network and File Shares

Network and cloud-managed file shares contained unencrypted sensitive documents including financial records, personally identifiable information, and internal security documentation accessible to standard

user accounts. Combined with weak password issues, any compromised account could access this data without additional privilege escalation.

Cloud Security (Azure Focused)

HIGH

Users Can Create Security Groups — Privilege Escalation Path

Azure Active Directory was configured to allow standard users to create security groups, establishing an uncontrolled privilege escalation path. An attacker with any valid account could create groups, add members, and potentially assign permissions to sensitive resources, bypassing the principle of least privilege and undermining role-based access control.

MODERATE

Key Vaults Accessible from Public Networks with RBAC Disabled

Azure Key Vaults storing cryptographic keys and secrets were accessible from public network endpoints and lacked Role-Based Access Control, relying instead on legacy vault access policies. This configuration exposes credential material to unauthorized access from any network position and lacks the granularity needed to enforce least-privilege access to secrets.

Web Application

HIGH

Insecure Direct Object Reference (IDOR) — Member PII Exposure

Member-facing web applications frequently contained an authorization flaw that allowed authenticated users to access other members' personal information by manipulating a sequential identifier in API requests. By iterating through numeric IDs, an attacker could systematically harvest names, email addresses, physical addresses, and phone numbers for every user in the system, a direct violation of data protection requirements under GLBA.

SaaS & Phishing

HIGH

SaaS Privilege Escalation — Self-Service Permission Elevation

Operational SaaS platforms were configured to allow users to elevate their own permissions, create new workspaces without approval, and share data externally without DLP controls. Complete SaaS integration with identity management platforms was inconsistent, facilitating numerous privilege escalation pathways for basic users of corporate purposed SaaS tools.

HIGH

No Phishing-Resistant MFA — Push-Notification Fatigue Vulnerability

Authentication relied heavily on push-notification MFA (Microsoft Authenticator) rather than phishing-resistant FIDO2/WebAuthn hardware tokens. Combined with inconsistent use of DMARC policies on the primary email domain, no formal security awareness training program, and no incident response plan, phishing resilience was critically low, vulnerable to credential harvesting through both technical and social engineering vectors.

Threat Modeling

CRITICAL

Hybrid Cloud Architecture — Three Critical Attack Scenarios Identified

Strategic threat modeling of hybrid IT infrastructures identified 16 threat scenarios across four threat actor categories. Three scenarios rated Critical: (1) phishing combined with uncontrolled file server exploitation could expose 3TB of unclassified organizational data, (2) the financial management system lacked MFA and could be compromised to access bank account and payment data, and (3) the Azure AD Connect synchronization pathway could be exploited to pivot between on-premises and cloud environments, achieving persistent access across the entire hybrid infrastructure.

CROSS-ENGAGEMENT TREND ANALYSIS

Conducting assessments across multiple organizations and security domains reveals patterns that single-point assessments cannot. The following trends emerged consistently, representing systemic, industry-wide challenges that credit unions must address through coordinated security programs rather than isolated remediation efforts.

4/4	4/4	9+
PHYSICAL ACCESS FAILURES	ORGS LACKING PHISHING-RESISTANT MFA	AD MISCONFIGURATIONS FOUND

1

Physical Security Controls Fail Under Adversarial Testing

Every organization tested had invested in physical security infrastructure — turnstiles, badge readers, CCTV, locked doors — yet assessors bypassed these controls at every location through social engineering and tailgating. The consistent pattern reveals that technical controls alone are insufficient without robust procedural enforcement, continuous visitor escorting, and regular adversarial validation.

2

Active Directory Remains the Crown Jewel — and the Weakest Link

Internal network assessments consistently revealed Active Directory environments with weak password policies, unmanaged service principal names, legacy protocols (SMBv1, NTLM), and insufficient monitoring. In every case, the assessment team achieved significant privilege escalation — in one engagement, reaching full Domain Administrator from an unauthenticated position within hours. These findings are universal across credit union environments that rely on on-premises Active Directory.

3

Cloud Security Posture Gaps Create Lateral Movement Paths

Azure environments consistently exhibited misconfigurations in identity management, network controls, and key management. Permissive security group creation, publicly accessible Key

Vaults, disabled RBAC, unencrypted disks, and missing activity log alerts created pathways for lateral movement between cloud and on-premises environments — particularly dangerous in hybrid architectures where Azure AD Connect synchronizes identity between domains.

4

SaaS Sprawl and Shadow IT Undermine Centralized Controls

Organizations relying on SaaS platforms for core operations faced consistent challenges with ungoverned data sprawl, self-service permission elevation, and inadequate audit logging. In one case, over 1,000 databases across 164 workspaces operated outside centralized governance. This pattern is endemic in credit unions adopting SaaS tools for member services, lending operations, and compliance workflows without corresponding security controls.

5

Phishing Resilience Is Overestimated Without Phishing-Resistant MFA

Every organization assessed relied on push-notification MFA or SMS codes rather than phishing-resistant FIDO2/WebAuthn tokens. Combined with gaps in email authentication (missing DMARC policies), absence of formal security awareness programs, and lack of incident response playbooks, organizations significantly overestimated their resilience to credential harvesting attacks — the #1 initial access vector targeting financial institutions.

6

Web Applications Expose Member Data Through Authorization Flaws

Member-facing web applications consistently contained authorization vulnerabilities — particularly Insecure Direct Object References (IDOR) — that could expose personally identifiable information at scale. These flaws bypassed otherwise well-implemented role-based access controls and session management, demonstrating that functional security controls do not guarantee authorization logic is correct.

CROSS-DOMAIN VULNERABILITY CHAINING

The most significant insight from a full-spectrum assessment is how vulnerabilities across independent domains combine to create compound attack scenarios with exponentially greater impact. Sidekick's methodology deliberately maps these cross-domain chains, the same approach real adversaries use, revealing risks that single-vector testing fundamentally cannot detect.

Full-Spectrum Attack Chain

Chain 1: Phishing to Full Domain Compromise

RECON	Attacker identifies the credit union's primary email domain lacks DMARC enforcement, enabling email spoofing. OSINT reveals employee names, roles, and email formats from public sources.
ENTRY	Spoofed phishing email targets employees with a credential harvesting page mimicking the Microsoft 365 login portal. Push-notification MFA (non-phishing-resistant) is bypassed through real-time proxy or MFA fatigue techniques.
ESCALATION	With valid credentials, the attacker accesses Azure AD and exploits permissive security group creation to elevate privileges. The attacker creates a security group, assigns it to sensitive resources, and accesses Key Vault secrets stored without RBAC enforcement.
PIVOT	Using Azure AD Connect synchronization, the attacker pivots to the on-premises Active Directory environment. Kerberoasting extracts service account hashes, and cracked credentials provide access to domain controllers. Shadow Credentials attack achieves Domain Administrator.
IMPACT	Full domain compromise enables access to network file shares containing unencrypted member PII, financial records, and operational data. The attacker has persistent access to both cloud and on-premises environments, with the ability to exfiltrate data, deploy ransomware, or maintain long-term access.

Chain 2: Physical Intrusion to Network Compromise

ENTRY	Attacker enters a branch location using an electrician pretext. Staff accept the cover story and provide access to restricted areas without verification. The attacker is left unsupervised in the server room.
IMPLANT	The attacker connects a rogue network device to an open Ethernet port in the server room, establishing a persistent backdoor to a C2 testing instance managed over Sidekick VPN. The rogue AP broadcasts on a wireless channel matching observed network baselines.
NETWORK	From the implant, the attacker performs null session enumeration against domain controllers, discovers user accounts, and executes a password spray using commonly observed weak credentials. Successful authentication provides a foothold on the internal network.
COMPROMISE	Kerberoasting extracts service account password hashes. With cracked service credentials and BloodHound-identified attack paths, the attacker escalates to Domain Administrator, gaining unrestricted access to all domain-joined systems, member databases, and financial applications.

Chain 3: SaaS Exploitation to Data Exfiltration

ENTRY	Attacker compromises an employee's SaaS platform credentials through phishing. The SaaS platform lacks integration with the organization's centralized identity provider, operating with local authentication and no MFA.
ESCALATION	The platform allows self-service permission elevation. The attacker creates a new workspace, grants themselves owner-level access, and invites an external email address controlled by the attacker — all without triggering audit alerts due to insufficient logging configuration.

DISCOVERY	Across 1,000+ databases and 164 workspaces, the attacker discovers sensitive operational data, member information, financial records, and internal security documentation. Public web views expose data externally without authentication.
IMPACT	Sensitive data is demonstrated that it can be exfiltrated through the SaaS platform's native export features. Because DLP controls are not enforced and audit logging was insufficient, the breach would go undetected until member data appears on the dark web, triggering regulatory notification requirements under GLBA.

Chain 4: Web Application to Member Account Takeover

RECON	Attacker identifies the credit union's member portal and creates a legitimate account. Analysis reveals that member profile endpoints use sequential numeric identifiers in API requests.
EXPLOIT	By manipulating the numeric ID parameter in the profile edit endpoint (IDOR vulnerability), the attacker systematically enumerates and retrieves personal information, names, email addresses, physical addresses, and phone numbers for every member in the system.
POISON	Simultaneously, the attacker exploits the web cache poisoning vulnerability by injecting a malicious X-Forwarded-Host header. Cached responses now contain references to an attacker-controlled domain, redirecting victims to a credential harvesting page.
IMPACT	Harvested member PII enables targeted spear-phishing campaigns against credit union members. Combined with the cache poisoning redirect, members visiting the legitimate website are served phishing content that captures banking credentials; a devastating combination of data exposure and credential theft.

WHY FULL-SPECTRUM CHAINING MATTERS

Each vulnerability in these chains might receive a "moderate" or "high" rating in isolation. But when chained across domains, they create realistic paths from a single phishing email to full organizational compromise in hours. Sidekick's methodology ensures these compound risks are identified, documented, and remediated as interconnected attack paths, not as disconnected findings scattered across separate reports.

This approach also highlights gaps around and the importance of monitoring and response capabilities that cut across specific technical or operational domains.

DEPLOYABLE REMEDIATIONS

Sidekick Security goes beyond identifying vulnerabilities, every engagement produces ready-to-deploy detection rules, policy templates, control mappings, and compliance documentation. These deliverables close the gap between "findings" and "fixed" immediately, rather than leaving organizations with a report and no clear path to remediation.

SIEM Detection Rules

Pre-built detection logic for each assessment domain: AD attack chain indicators (Kerberoasting, DCSync, Golden Ticket), Azure suspicious sign-in patterns, web application authorization abuse, physical access anomalies, and SaaS data exfiltration triggers, tailored to the client's specific SIEM platform.

WAF & Network Rules

Custom WAF rules for web application protection including IDOR prevention patterns, cache poisoning mitigation, and host header validation. Network-level rules for SMB signing enforcement, NTLM restriction, and rogue device detection.

Detection & Response Strategy

Phased enhancement plan (0–30, 31–90, 91–180 days) covering detection logic deployment, SOC workflow integration, incident response playbook development, and continuous monitoring implementation across all assessment domains.

Control Mappings

Direct mapping of every finding to applicable regulatory controls (NCUA Part 748, GLBA, PCI-DSS, NIST CSF, SOC 2 TSC, ISO 27001) with gap analysis, remediation priority scoring, and audit-ready documentation.

GRC Impact Analysis

Comprehensive governance, risk, and compliance impact assessment documenting how each finding affects regulatory standing, risk register entries, board-level reporting requirements, and examination preparedness.

Remediation Roadmap

Prioritized 30/60/90-day remediation plan with quick wins, medium-term improvements, and strategic enhancements calibrated to organizational capacity, regulatory timelines, and risk severity.

Cloud Hardening Playbook

Azure-specific hardening guidance covering security group restrictions, Key Vault RBAC migration, CMK encryption deployment, activity log alert configuration, network security group tightening, and Azure AD Conditional Access policies.

AD Hardening & Monitoring

Active Directory remediation package including password policy enforcement, SPN audit and cleanup, tiered administration model design, Shadow Credentials prevention, SMB signing enforcement, and privileged access monitoring rules.

Detection Rule Examples

The following illustrate the type of deployable detection logic Sidekick delivers as part of every engagement. Rules are tailored to the client's specific SIEM platform, log sources, and operational context.

Network — Kerberoasting Detection

Rule Name	AD-001: Kerberoasting — Anomalous TGS Requests
Trigger	Single user account requests TGS tickets for 3+ service accounts within a 10-minute window; OR any TGS request using RC4 encryption (etype 0x17)
Data Sources	Windows Security Event Log (Event ID 4769), Domain Controller audit logs
Severity	High (escalate to Critical if targeting privileged service accounts)
Response	Alert SOC, isolate requesting account, audit targeted SPNs, check for credential exposure

Cloud — Azure Security Group Manipulation

Rule Name	AZ-001: Unauthorized Security Group Creation
Trigger	Non-admin user creates a new security group in Azure AD; OR security group membership changes by non-privileged account; OR new group assigned to Key Vault or storage account access policy
Data Sources	Azure AD Audit Logs, Azure Activity Logs, Microsoft Sentinel
Severity	Medium (escalate to High if group gains access to Key Vault or sensitive resources)
Response	Alert security team, review group membership and assigned permissions, verify business justification

Application — IDOR Exploitation Detection

Rule Name	APP-001: Sequential ID Enumeration — Potential IDOR
Trigger	Single authenticated session requests 10+ consecutive sequential resource IDs within 5 minutes; OR single session accesses resources belonging to 5+ distinct users
Data Sources	Web application access logs, WAF logs, API gateway telemetry
Severity	High (immediate escalation — potential mass PII exposure)
Response	Block session, alert incident response, audit accessed records for breach notification assessment

GRC Impact Summary

Every engagement produces comprehensive compliance documentation mapping findings to applicable regulatory frameworks. This helps our customers not only close real gaps, but stay prepared for regulatory and external audits that put pressure on the team. The table below demonstrates how Sidekick contextualizes findings from all assessment domains within the regulatory environment specific to credit unions and financial institutions.

FRAMEWORK	CONTROL	FINDING IMPACT	REMEDIATION
NCUA Part 748	Info Security Program	Physical access failures, AD compromise, and cloud misconfigurations demonstrate gaps in safeguards for member data	Full-spectrum remediation across physical, network, cloud, and application layers
GLBA Safeguards	Physical & Technical	IDOR exposing member PII, unencrypted network shares, and SaaS data sprawl violate safeguard requirements	Authorization fixes, DLP controls, data classification, and encryption enforcement
PCI-DSS	Req 6, 8, 9, 10	Web app flaws (Req 6), weak MFA (Req 8), physical access failures (Req 9), insufficient logging (Req 10)	Application patching, FIDO2 MFA, physical controls, and comprehensive audit logging
NIST CSF	ID, PR, DE, RS	Incomplete asset inventory (ID), access control gaps (PR), detection blind spots (DE), no IR plan (RS)	Asset discovery, tiered access model, SIEM detection rules, and IR playbook
SOC 2	CC6, CC7, CC8	Logical access (CC6), system operations (CC7), and change management (CC8) control deficiencies	RBAC enforcement, monitoring deployment, and change control process implementation

ISO 27001	A.9, A.12, A.13	Access control (A.9), operations security (A.12), and communications security (A.13) nonconformities	Policy updates, technical controls, and continuous monitoring framework

VSEC: CONTINUOUS SECURITY PARTNERSHIP

> *A penetration test report identifies the gaps. vSec closes them. Sidekick's vSec subscription service embeds our engineers and security leaders directly with your team to accelerate remediation, build program maturity, and transform findings into measurable security improvements…not just a report on a shelf.*

Most organizations complete a penetration test, receive a report full of critical findings, and then face the challenge of actually fixing what was found, often without the specialized expertise, bandwidth, or strategic context needed to prioritize and execute effectively. Findings sit in a backlog. Compliance deadlines approach. The same vulnerabilities reappear in the next assessment.

Sidekick's vSec subscription service breaks this cycle by embedding Sidekick engineers and security leaders directly with the customer's team immediately after an engagement. vSec is not staff augmentation, it's a strategic partnership that brings the same expertise that found the vulnerabilities to the work of closing them.

What vSec Delivers

Hands-On Remediation

Sidekick engineers work side-by-side with your team to implement fixes, from AD hardening and Azure security group lockdown to WAF rule deployment and SIEM detection logic tuning. We don't just advise; we execute.

Security Program Development

Our leadership team partners with your CISO and security leadership to build and mature your overall security program, developing policies, governance frameworks, risk management processes, and board-level reporting that demonstrates measurable improvement.

Continuous Validation

As remediations are implemented, Sidekick validates their effectiveness through targeted retesting, confirming that fixes actually work under adversarial conditions rather than just checking a compliance box.

Knowledge Transfer

Every vSec engagement includes structured knowledge transfer to ensure your team develops the internal capability to maintain and extend the security improvements after the engagement concludes. We build capacity, not dependency.

vSec Example Engagement Model

PHASE 1	PHASE 2	PHASE 3	PHASE 4
0–30 Days	**31–90 Days**	**91–180 Days**	**Ongoing**
Critical remediation triage. Deploy quick wins from assessment findings. SIEM detection rules go live. AD password policy enforcement.	Infrastructure hardening. Azure RBAC migration. Cloud security posture remediation. Web application authorization fixes deployed.	Program maturity. FIDO2 MFA rollout. SaaS governance framework. Formal IR plan development. Security awareness program launch.	Continuous partnership. Retesting and validation. Board reporting support. Regulatory examination preparation. Emerging threat advisories.

THE VSEC DIFFERENCE

Traditional consulting engagements end with a report. Sidekick's vSec model starts where the report ends. By embedding the same experts who conducted the assessment directly into remediation, we eliminate the knowledge loss, context switching, and re-explanation that plague traditional handoff models. The engineers who found the Domain Admin path are the same ones who lock it down.

BUSINESS IMPACT & RESULTS

The combined findings from full-spectrum assessment demonstrate the transformative value of evaluating security holistically across every domain. Organizations that act on these results move from a posture of assumed security to one of validated, measurable resilience with clear paths to continuous improvement through the vSec partnership model.

BEFORE SIDEKICK

- Physical controls assumed effective but never adversarially tested
- Active Directory attack paths unknown and unmonitored
- Cloud security posture unvalidated across Azure environments
- Web application authorization logic untested at the API level
- SaaS sprawl growing without governance or visibility
- Phishing resilience overestimated — no phishing-resistant MFA
- Compliance gaps unknown with no cross-framework mapping
- No detection rules for cross-domain attack indicators

AFTER SIDEKICK

- Validated security posture across all seven assessment domains
- AD attack paths mapped with hardening and monitoring deployed
- Azure security posture remediated with RBAC and encryption
- Authorization flaws fixed with WAF rules and API-level controls
- SaaS governance framework with DLP and audit logging
- FIDO2 MFA roadmap with phishing-resistant authentication
- Full regulatory compliance mapping across 6 frameworks
- Deployable detection rules and incident response playbooks

Client Perspective

> *"The depth of Sidekick's assessment went far beyond what we've experienced with traditional penetration testing firms. They didn't just find issues that we knew about, they showed us exactly how an attacker would string them all together and cause real problems. Everything the team delivered along with the report evolved this experience way beyond our annual pentest."*
>
> **— Chief Information Security Officer, Financial Services Organization**

WHY SIDEKICK SECURITY?

Sidekick Security delivers a fundamentally different approach to security assessment, designed by a former CISO and Red Teamer. One built on full-spectrum adversarial methodology, cross-domain intelligence, deployable outcomes, and a continuous partnership model that ensures findings become fixes.

Full-Spectrum Methodology

We assess every domain an attacker would target — physical, network, cloud, application, SaaS, phishing, and organizational architecture — because real adversaries don't limit themselves to one attack vector. Single-domain testing leaves compound risks invisible.

Cross-Domain Attack Chaining

Our methodology deliberately maps how vulnerabilities across independent domains combine into compound attack scenarios. The path from a phishing email to Domain Admin to member data exfiltration, that's the risk organizations need to understand.

Deployable Remediations

Every engagement delivers more than a report. SIEM rules, WAF configurations, IR playbooks, compliance mappings, and hardening guides, ready to deploy immediately. We close the gap between "findings" and "fixed."

vSec Partnership Model

Our vSec subscription service embeds Sidekick engineers directly with your team after each engagement. The same experts who found the vulnerabilities help close them, accelerating remediation, building internal capability, and eliminating the knowledge loss of traditional consulting handoffs.

Financial Services Expertise

Our team has deep experience in the credit union and banking sector. We understand NCUA examination expectations, GLBA requirements, and the unique challenges facing institutions with distributed branches, hybrid cloud, and member-facing applications.

Multi-Engagement Intelligence

By assessing organizations across the financial services sector, we bring cross-industry trend insights that help clients benchmark their security posture against peer institutions and prioritize investments where they matter most.

READY TO SEE YOUR FULL ATTACK SURFACE?

Contact Sidekick Security to discuss how our full-spectrum assessment methodology and vSec partnership model can strengthen your organization's security posture, close gaps faster, and build lasting program maturity.

hello@sidekicksecurity.io | sidekicksecurity.io