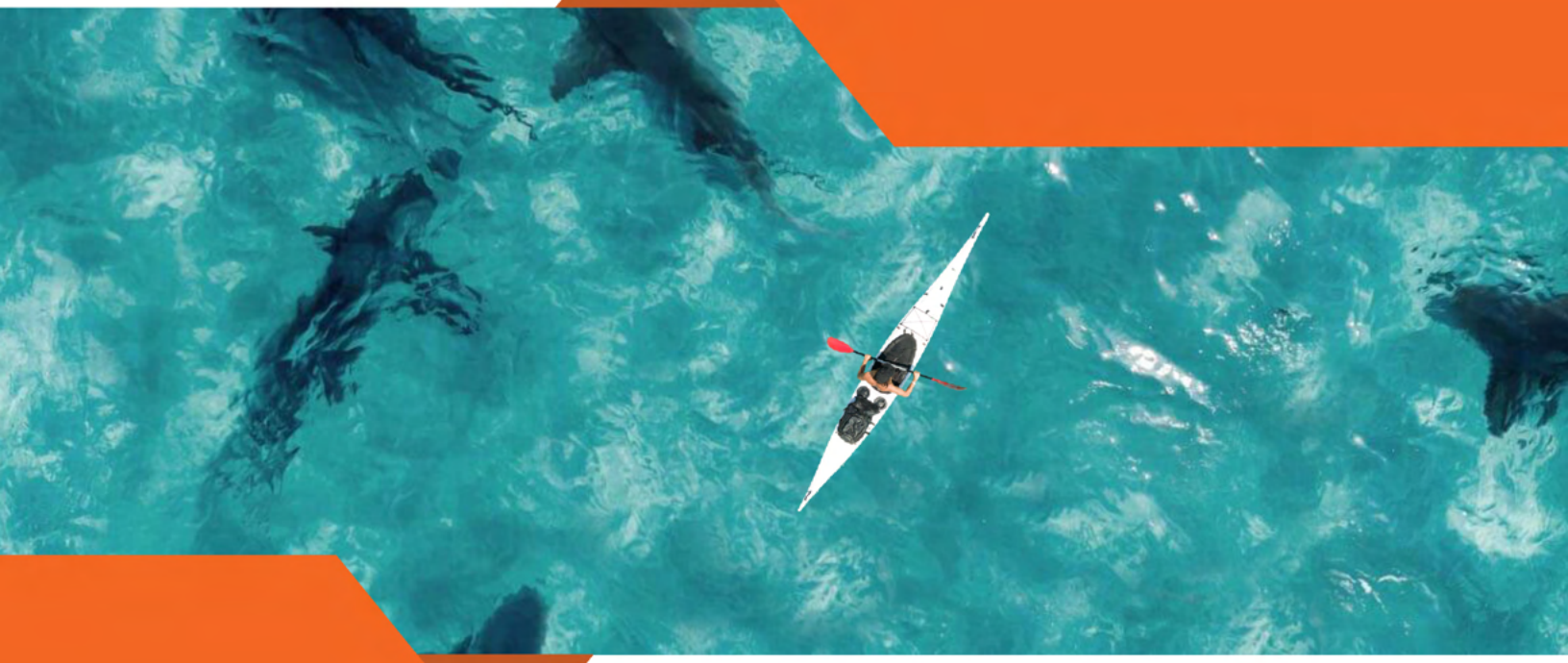


CYBERSECURITY SOLUTIONS FOR CREDIT UNIONS

Safeguarding Member Accounts, Financial Transactions, & Brand Reputation

SPECIALIZED S|3 SECURITY SERVICES

CYBERSECURITY IN CREDIT UNIONS

IIn the financial industry, trust is non-negotiable. Whether offering savings, lending, or digital banking services, credit unions must ensure secure transactions, uninterrupted access, and protection of their members' most sensitive data. As digital transformation accelerates, it also introduces new attack surfaces and regulatory responsibilities.

With high-value member data, complex IT ecosystems, and constant exposure to cyber threats, credit unions must take proactive steps to safeguard operations, reinforce member confidence, and protect institutional integrity.

At S3 Security, we provide end-to-end support—helping you understand your risks, apply the right strategies, guide implementation, and remain a trusted partner through deployment and beyond.

© 2025 Specialized Security Services, Inc. All Rights Reserved

WHY SPECIALIZED SECURITY SERVICES, INC. (S3 SECURITY)?

For more than 25 years, S3 Security has been the trusted cybersecurity partner for mission-driven, member-focused institutions like credit unions. We don't just deliver solutions; we build lasting relationships. As a full-service cybersecurity firm, we operate as an extension of your team, helping you protect member trust, financial assets, and operational resilience.

Whether you need support identifying risk, implementing controls, or responding to incidents, we deliver everything from assessments to remediation, plus project management and strategic staffing to ensure success.

Our support spans the entire journey: from education and planning to implementation, management, and long-term partnership.

- ✓ **Founder-owned and independently operated –** We answer only to our clients, not investors.
- ✓ **One-stop cybersecurity partner –** From risk assessments and penetration testing to regulatory readiness, remediation, and staff augmentation—we've got you covered.
- ✓ **Long-lasting client partnerships –** Many of our clients have been with us for decades.
- **Industry-leading expertise –** Our team understands the unique regulatory and operational challenges credit unions face.
- ✓ **Custom-tailored security programs –** Designed to fit your institution's structure, systems, and compliance obligations, not generic one-size-fits-all
- ✓ approaches.
- **Proactive, not reactive –** We detect and eliminate threats before they
- ✓ impact your members or operations.

Join the growing number of credit unions that trust S3 Security to protect member data, institutional reputation, and regulatory standing—today and for the future.

© 2025 Specialized Security Services, Inc. All Rights Reserved

KEY CYBERSECURITY CHALLENGES IN FINANCE

Member trust is built with each login, transaction, and statement—but can be lost in an instant when systems are compromised. In today's financial environment, protecting that trust is critical to preserving your institution's reputation, regulatory standing, and long-term member relationships.

Core Banking & Financial System Vulnerabilities

Core systems manage deposits, loans, transfers, and member records, making them high-value targets for attackers. Misconfigurations, legacy software, or weak controls can expose critical data and disrupt operations.

Phishing & Social Engineering Attacks

Employees and executives are prime targets for phishing campaigns and impersonation attacks aimed at accessing sensitive data, redirecting funds, or deploying ransomware.

Branch & Location Consistency

Maintaining standardized security policies across branches, departments, and business units is an ongoing challenge. Disparities in security maturity and enforcement can expose the entire institution to systemic risk.

Payment System & ATM Vulnerabilities

Payment processing platforms and ATMs are frequent targets for card skimming, malware, and data exfiltration. Weak endpoint security or outdated protocols leave systems open to exploitation.

Cloud & IoT Security

Cloud platforms and IoT-connected devices like smart ATMs and surveillance systems expand the attack surface. Without strong access controls and monitoring, they introduce critical vulnerabilities.

Third-Party Vendor Risks

As credit unions adopt cloud solutions and outsource critical operations, the security posture of vendors becomes a shared risk. Without rigorous controls, third-party vulnerabilities can lead to breaches in your environment.

Compliance & Regulatory Requirements

Credit unions must comply with complex regulatory mandates such as GLBA, PCI DSS, NCUA regulations, FFIEC guidelines, and more. Noncompliance can lead to costly penalties, reputational harm, and operational disruptions.

Ransomware & Data Breaches

Financial data is among the most lucrative for cybercriminals. Ransomware attacks can cripple systems, lock down member accounts, and trigger mandatory data breach disclosures.

The question isn't if an attack will happen, but when.

Are you prepared?

© 2025 Specialized Security Services, Inc. All Rights Reserved

COMPLIANCE & RISK ASSESSMENTS

Ensuring compliance with financial regulations and cybersecurity best practices is essential for avoiding regulatory penalties and protecting member data.

- **FFIEC, FDICIA IT Audit**
- **SOC 2 Readiness & Compliance Assessments**
- **PCI DSS Assessments** (Payment Card Industry Data Security Standard)
- **SWIFT Customer Security Program (CSP) Assessments**
- **NACHA Rules Compliance Reviews**
- **GDPR, CCPA, & Other Privacy Compliance Reviews**
- **ISO 27001 Information Security Audits**
- **NIST Cybersecurity Framework Assessments**
- **Third-Party Vendor Risk Assessments**
- **Cybersecurity Maturity Assessments for Financial Institutions**
- **Security Awareness Training**
- **Member Risk Assessments**

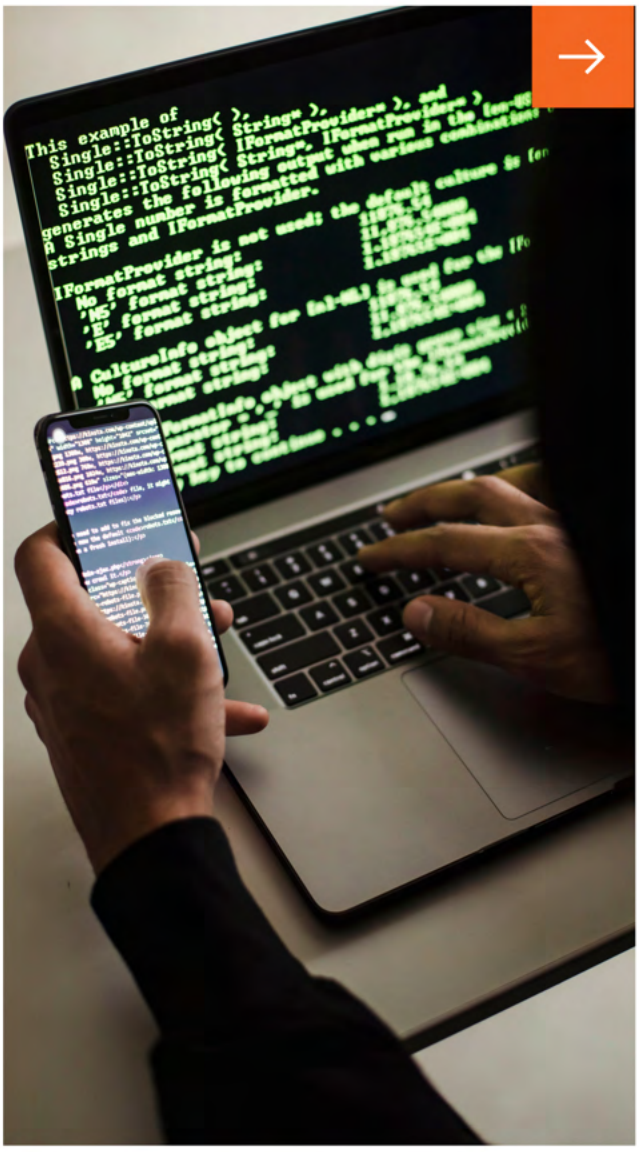
BENEFIT

Stay compliant, reduce regulatory exposure, and reinforce member trust in your institution's security posture.

© 2025 Specialized Security Services, Inc. All Rights Reserved

PENETRATION TESTING & VULNERABILITY MANAGEMENT

Identifying and addressing security weaknesses before cybercriminals can exploit them.



- **Core Banking, ATM & Payment System Penetration Testing**
- **Mobile Banking & Online Platform Security Testing**
- **Web Application & Network Vulnerability Scanning**
- **API & Cloud Security Assessments**
- **Wireless Network & Guest Wi-Fi Security Testing**
- **Dark Web & Open-Source Intelligence (OSINT) Monitoring**
- **Ransomware Simulation & Incident Response Testing**

BENEFIT

Prevent costly cyberattacks, protect sensitive data, and ensure secure, uninterrupted member services.

© 2025 Specialized Security Services, Inc. All Rights Reserved

DATA PROTECTION & PRIVACY

Safeguarding member information and sensitive financial data against unauthorized access, misuse, and theft.

- **GLBA Compliance & Safeguards Rule Implementation**
- **NCUA Member Risk Assessment**
- **Secure Encryption for Financial Transactions & Member Data**
- **Data Loss Prevention (DLP) Programs**
- **Privacy Impact Assessments (PIAs)**
- **Data Governance & Retention Policies Aligned with FFIEC, NIST & ISO Standards**
- **Network Segmentation & Role-Based Access for Confidential Data**

BENEFIT

Build member trust and meet regulatory expectations by ensuring sensitive data is secured and managed responsibly.

© 2025 Specialized Security Services, Inc. All Rights Reserved

INCIDENT RESPONSE & BUSINESS CONTINUITY

Minimizing operational disruption, financial loss, and reputational damage during a cyber incident.

- **Incident Response Planning & Tabletop Exercises**
- **Disaster Recovery & Ransomware Resilience Strategies**
- **Business Continuity Strategies & Testing**
- **Disaster Recovery Aligned with Financial Regulatory Expectations**
- **Crisis Management & Communication Planning**

BENEFIT

Minimize downtime, protect critical financial operations, and maintain member confidence—even in the face of disruption.

© 2025 Specialized Security Services, Inc. All Rights Reserved

PROFESSIONAL CYBERSECURITY CONSULTING

Strategic guidance to enhance your security posture, reduce regulatory risk, and protect your institution's reputation.

- **Virtual CISO (vCISO) Services**
- **Staff Augmentation**
- **Cyber Risk Management & Governance**
- **Remediation Management & Assistance**
- **Security Policy & Procedure Development**
- **Secure Cloud & Fintech Technology Strategies**
- **Brand Protection Against Cyber Threats**
- **Member & Employee Identity Theft Prevention Strategies**
- **Security Awareness Training**

BENEFIT

Access executive-level cybersecurity leadership and specialized expertise—without the overhead of a full in-house team.

© 2025 Specialized Security Services, Inc. All Rights Reserved

WHY LEADING CREDIT UNIONS TRUST S3 SECURITY

Credit Union Expertise

We understand credit unions' unique cybersecurity and compliance challenges and help them navigate member-focused security and regulations with confidence.

Proven Track Record

With over 25 years of experience in high-risk industries, we've helped credit unions navigate evolving threats and meet stringent regulatory demands.

Custom-Tailored Programs

No one-size-fits-all solutions. Our strategies are built to align with your systems, risk profile, and business objectives.

Proactive Risk & Compliance Management

From FFIEC and FDICIA to GLBA, NCUA, PCI DSS, and SOC 2, and we help you meet complex regulatory requirements while minimizing business risk and exposure.

Resilient, Business-Centric Security

We focus on prevention, continuity, and long-term resilience, keeping your operations protected and your members confident.

Trusted by Partner for Credit Unions

Credit unions rely on us for expert guidance and long-term partnership to protect their members and operations.

PARTNER WITH S3 SECURITY TO PROTECT YOUR FINANCIAL INSTITUTION

The most successful credit unions don't just react to cyber threats—they prevent them. With S3 Security as your cybersecurity partner, you can protect your business, your members, and your reputation from digital risks without disruption.

Let us help you create a secure and seamless experience for your members.

© 2025 Specialized Security Services, Inc. All Rights Reserved

GETTING STARTED - ESTABLISHING YOUR CYBERSECURITY BASELINE

Every successful cybersecurity program begins with a strong understanding of your current environment. At S3 Security, our initial engagement recommendations are designed to provide a clear picture of your cybersecurity posture, regulatory gaps, and data exposure. These foundational steps help us align with your operational priorities, address critical risks, and chart a path toward long-term resilience.

In the first 6–8 weeks, we recommend the following assessments:

- **Penetration Testing** – Internal, external, web application, website, API, and cloud testing to identify exploitable vulnerabilities before attackers do.
- **Vulnerability Assessment** – Internal and external scans to detect system weaknesses and misconfigurations.
- **Enterprise Cybersecurity Gap Assessment** – A comprehensive evaluation mapped to FFIEC, FDICIA, GLBA, NCUA, PCI DSS, SOC 2, and other regulatory requirements to assess current compliance and control maturity.
- **Enterprise Data Discovery** – Locate and analyze sensitive member and financial data that may be improperly stored, unencrypted, or accessible beyond policy.
- **Ransomware Simulation** – Evaluate your organization's ability to detect, respond to, and recover from a simulated ransomware attack.

For each of these milestones, S3 Security will deliver an Executive Summary and Detailed Findings Report, complete with prioritized recommendations and a custom project plan.

We will collaborate closely with your team to develop a tailored remediation strategy that reduces your risk and strengthens your defenses.

© 2025 Specialized Security Services, Inc. All Rights Reserved

ONGOING PROGRAM & STRATEGIC GUIDANCE

8 Weeks & Beyond:

Following the initial assessments, S3 Security continues to support your institution with strategic guidance and expert execution to strengthen cybersecurity over time. This may include:

- Ongoing remediation management and technical advisory services.
- Staff augmentation to support internal security, compliance, or IT teams.
- Deployment of long-term security services with recommended testing and review frequencies.
- Ongoing compliance readiness aligned with FFIEC, FDICIA, GLBA, NCUA, PCI DSS, SOC 2, and other regulatory requirements.

A PARTNERSHIP BUILT FOR THE LONG HAUL

Let's build your foundation for long-term cybersecurity success.

With S3 Security, you're not just checking boxes. You're investing in a trusted partner dedicated to your organization's resilience, reputation, and competitive edge. Our goal is to equip your team with the insights, tools, and support needed to confidently navigate today's threats and tomorrow's challenges.

© 2025 Specialized Security Services, Inc. All Rights Reserved

YOUR CYBERSECURITY PARTNER

S|3 SPECIALIZED SECURITY SERVICES

FLOAT ON

Cybersecurity and compliance to ward off any threat.

Wherever You Are in Your Cybersecurity Journey—We're With You

At S3 Security, we meet you where you are, whether you're just beginning to assess risk or advancing a mature security program. We understand the complexities you face, and we know that one of the greatest benefits of strong compliance and cybersecurity practices is lasting peace of mind.

Our mission is to strengthen your organization's resilience, efficiency, and long-term success by aligning security strategies with your business goals.

With decades of experience guiding clients through evolving regulatory requirements and emerging threats, we are your trusted partner in navigating the ever-changing technology and compliance landscape.

CONTACT US

SPECIALIZED SECURITY SERVICES, INC.
4975 Preston Park Blvd., Suite 510
Plano, TX 75093
972-378-5554 | info@s3security.com
www.s3security.com

© 2025 Specialized Security Services, Inc. All Rights Reserved