CSA VULNERABILITY SCANNING SERVICES BRIEF

Reveal Risks. Guide Decisions. Build Resilience.

SPECIALIZED S|3 SECURITY SERVICES

VULNERABILITY SCANNING SERVICES

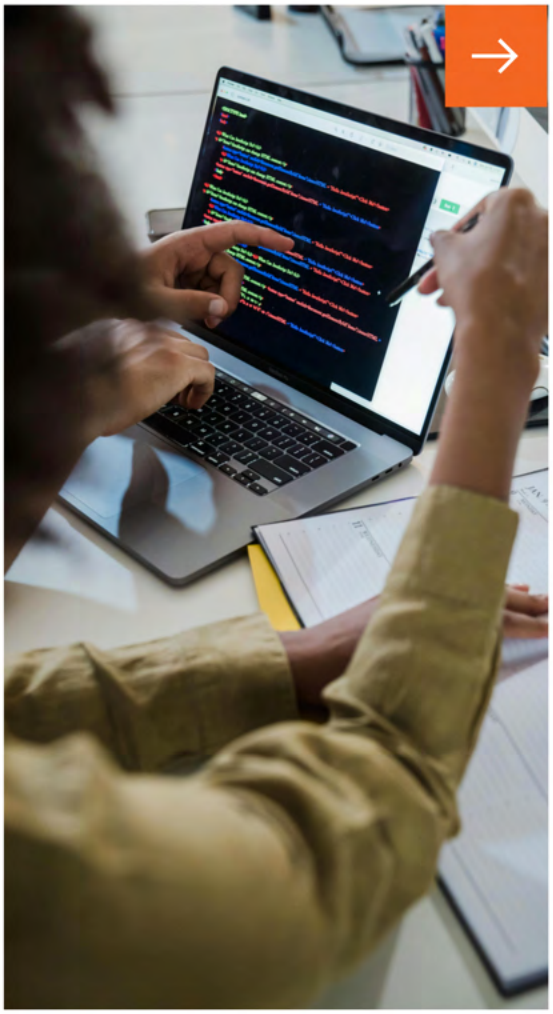
See What Others Miss. Strengthen What Matters Most.

Cybersecurity begins with visibility, and visibility begins with scanning. Vulnerability scans uncover weaknesses that attackers can exploit, insiders can misuse, or busy teams may overlook. At Specialized Security Services, Inc. (S3 Security), we deliver certified, framework-aligned scanning services that expose misconfigurations, unpatched systems, unauthorized access points, and exploitable vulnerabilities across your infrastructure.

Whether you're addressing compliance requirements, supporting a risk-based security strategy, or preparing for an audit, S3 Security helps you detect exposure early — so you can prioritize action with confidence.

EXPERTISE YOU CAN TRUST

With over 25 years of cybersecurity experience, S3 Security supports organizations across highly regulated industries and fast-evolving threat landscapes. Our scanning services align with trusted frameworks like CMMC, HIPAA, ISO, and NIST. We give you visibility into your current risk posture and provide clarity on how to strengthen it.



TAILORED TO YOUR BUSINESS

No two environments are the same. We adapt each engagement to your architecture, business priorities, and risk profile. Whether your infrastructure is on-premises, in the cloud, or hybrid, we help define the right scope and scan with minimal disruption to operations.

MORE THAN A SCAN – A STRATEGIC TOOL

We do more than run scans. We help you act on the results. Reports are designed for both technical and executive stakeholders, providing business-aligned, actionable insight to support remediation, planning, and regulatory response. You can expect expert validation, quality assurance, and clear guidance instead of a raw data dump.

Clarity drives better decisions. Visibility enables resilience.

© 2025 Specialized Security Services, Inc. All Rights Reserved

CERTIFIED EXPERTS & PROVEN TOOLS

Leading organizations trust S3 Security for scanning solutions that combine deep cybersecurity expertise with certified compliance knowledge. We do more than run tools. We apply them with precision to deliver clear, defensible insights that strengthen your security posture and support strategic goals.

Our vulnerability scanning services align to trusted cybersecurity frameworks including CMMC, HIPAA, ISO 27001, and NIST. We use certified platforms and proven methodologies to deliver consistent, reliable results your team can act on with confidence.

FRAMEWORKS & METHODOLOGIES

We align our scanning to standards that meet your operational and compliance goals:

- **Compliance-Driven:** CMMC, HIPAA, ISO, NIST
- **Risk-Aligned:** MITRE ATT&CK, CVSS, CWE
- **Governance-Supported:** Vulnerability management best practices, executive-ready reporting

Scanning only adds value when it leads to action. Our expert team helps you identify which vulnerabilities pose real risk and provides clear guidance on how to fix them before they can be exploited.

© 2025 Specialized Security Services, Inc. All Rights Reserved

TECHNICAL CAPABILITIES

S3 Security delivers enterprise-grade vulnerability scanning across a wide range of environments, assets, and organizational requirements. Our team combines certified expertise, advanced platforms, and proven methodologies to help you identify and manage weaknesses before they can be exploited. Below are key areas of focus:

External Vulnerability Scanning

We assess internet-facing systems to identify exposures that attackers can discover and exploit, including unpatched systems, open ports, misconfigured services, and weak SSL/TLS settings. External scanning provides visibility into your perimeter and helps reduce the risk of exploitation before threats reach internal systems.

Internal Vulnerability Scanning

We scan internal networks to uncover weaknesses often exploited by malicious insiders or attackers who bypass perimeter defenses. This includes outdated operating systems, missing patches, excessive permissions, and vulnerable services. These scans support security best practices and compliance readiness for frameworks such as CMMC, HIPAA, ISO, and NIST.

URL/URI/FQDN Scanning

We scan public-facing URLs, URIs, and fully qualified domain names (FQDNs) to identify exposed services, outdated software, insecure configurations, and other vulnerabilities accessible from the internet. These assets are often overlooked but can serve as entry points for attackers if not regularly tested and secured.

Application and API Scanning

We conduct authenticated and unauthenticated scans of web applications and APIs to identify OWASP Top 10 risks such as SQL injection, XSS, and insecure logic. Scanning includes internal, external, and third-party applications, with an emphasis on both dynamic behavior and known code-level exposures.

Cloud Environments

Our services extend to public, private, and hybrid cloud deployments. We identify misconfigured security settings, exposed cloud services, and asset-specific vulnerabilities across distributed and dynamic environments.

Actionable Reporting

All scan results are delivered in a business-aligned format that includes severity, asset impact, remediation guidance, and summary reporting for both technical and executive stakeholders. Reports support continuous security improvement, audit preparation, and alignment with frameworks such as HIPAA, ISO, CMMC, and NIST.

Visibility leads to control. Prioritized insight leads to action.

© 2025 Specialized Security Services, Inc. All Rights Reserved

OUR VULNERABILITY SCANNING METHODOLOGY

Effective scanning requires more than automation. Our structured approach combines expert guidance with actionable results to reduce disruption, accelerate remediation, and strengthen your defenses.

1

Planning & Scoping

We begin by validating the scan scope in coordination with your team. This includes internal and external components such as IP ranges, domains, cloud assets, and web applications. Timing is coordinated to minimize operational disruption and avoid scanning during sensitive periods.

2

Vulnerability Scanning

Our engineers conduct external and internal scans using certified tools and proven techniques. We identify outdated components, insecure configurations, missing patches, and exposed services that pose a real threat to your environment.

3

Analysis & Risk Prioritization

Findings are reviewed using CVSS scoring and threat intelligence to assess severity, exploitability, and business impact. We prioritize vulnerabilities that represent the highest risk and provide clear guidance to help your team take informed, effective action.

4

Initial Reporting

We deliver clear, organized reports tailored to both technical and executive stakeholders. Deliverables include an Executive Summary, Detailed Findings with remediation guidance, and a Scan Workbook for tracking. Reports are designed to support planning, communication, and measurable progress.

5

Rescanning & Attestation

After remediation is complete, we perform a follow-up scan to confirm that vulnerabilities have been resolved. If validation criteria are met, we issue an Attestation of Scan Completion (AOSC) to support internal documentation, compliance initiatives, or external reporting.

Strong cybersecurity starts with structured scans, prioritized findings, and expert guidance you can trust.

© 2025 Specialized Security Services, Inc. All Rights Reserved

MEASURING WHAT MATTERS

What Does a Scan Reveal?

Vulnerability scans uncover weaknesses that attackers could exploit, such as unpatched software, outdated protocols, exposed services, and misconfigurations. These issues may not indicate an active breach, but they expose pathways that could lead to one. Identifying and prioritizing these exposures helps your team take focused, preventive action.

Risk Severity Ratings

We rank all findings by severity so your team knows what to fix first. Using established scoring systems like CVSS and OWASP, we assess the likelihood, impact, and urgency of each vulnerability. This provides a consistent, defensible view of risk across your environment and helps you prioritize remediation efforts that address real threats to your organization.

Risk Level	NVD CVSS v3	OWASP Score	Definition
Critical	9.0–10.0	9.0–10.0	Immediate, system-wide risk with potential for full compromise and data loss. Often systemic in nature.
High	7.0–8.9	6.0–8.9	Serious vulnerabilities that may lead to sensitive data exposure or administrative access.
Medium	4.0–6.9	3.0–5.9	Issues that require chaining or elevated privileges to exploit, with moderate business impact.
Low	0.1–3.9	0.1–2.9	Minimal impact vulnerabilities unlikely to result in significant harm.
Informational	0.0	0.0	No direct risk, but useful for awareness and best practices.

Know the impact. Prioritize what matters.

Our reports highlight the vulnerabilities that pose real risk. Each finding includes business context, potential impact, and clear remediation guidance so your team can act quickly and effectively.

© 2025 Specialized Security Services, Inc. All Rights Reserved

A BETTER SCANNING EXPERIENCE

At S3 Security, we understand that how your vulnerability scans are managed has a direct impact on your security operations and strategic outcomes. That's why we provide a dedicated engagement team to keep your scanning program organized, proactive, and on track. Your team can stay focused on protecting the business, not chasing paperwork.

What You Can Expect:

- A dedicated Client Administrator (CA) to oversee scheduling & coordination
- Proactive communication from kickoff through reporting
- Clear expectations & timelines for each scan
- Scope & IP address submission guidance
- Ongoing reminders to support compliance deadlines

From agenda calls to report delivery, every step is designed to ensure a smooth, transparent, and high-quality experience.

BUILT-IN QUALITY ASSURANCE

Our QA process ensures every report meets your expectations and supports internal review needs. Each deliverable is reviewed for clarity, completeness, and actionability before final delivery.

S3 Security QA Process:

- **Engineering QA** – Validation by an experienced cybersecurity engineer
- **VP Review** – Review for completeness and content structure
- **Executive Review** – Final approval by EVP/CTO
- **Delivery QA** – Final check by Business Operations prior to delivery

Every scan report we deliver is held to the highest standard: accurate, defensible, and ready to support your next decision.

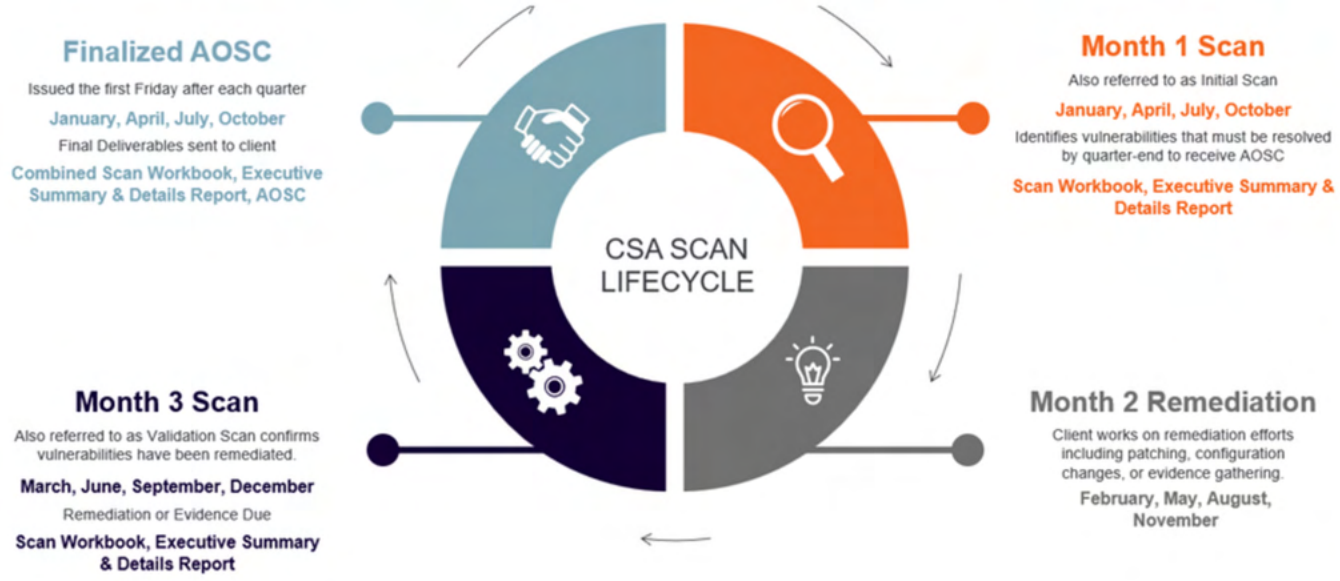
© 2025 Specialized Security Services, Inc. All Rights Reserved

WHAT TO EXPECT DURING YOUR CSA SCANNING ENGAGEMENT

Consistent scanning. Clear timelines. Confident execution.

We manage CSA scanning with a structured quarterly process designed to reduce disruption and improve risk visibility. From initial discovery to final reporting, our scanning engineers and delivery team support you with clear timelines, validated deliverables, and proactive scheduling to keep your program moving forward.

QUARTERLY CSA SCAN TIMELINE & DELIVERABLES



Your Scan Support Team

Each engagement is guided by a cross-functional team:

- **Client Administrator:** Coordinates schedules and logistics
- **Scanning Engineers:** Perform vulnerability scans and remediation guidance
- **Delivery Team:** Finalizes deliverables including the AOSC

Every step is built to reduce disruption, increase visibility, and give you clarity on timelines, deliverables, and what happens next.

Clear roles. Smooth execution. Strong results.

© 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

Whether you're strengthening internal defenses, preparing for an audit, or building a proactive risk management strategy, S3 Security is here to help. Our CSA Scanning Services give you clear visibility into your environment, empowering your team to act with confidence. We bring clarity to complexity and peace of mind to decision-makers.

Our mission is to reduce risk, build resilience, and help you stay ahead of evolving threats through cybersecurity strategies tailored to your business goals.

With over 25 years of experience helping clients secure their environments, protect their reputation, and meet regulatory expectations, S3 Security is your trusted partner for vulnerability insight, remediation planning, and strategic cybersecurity support.

CONTACT US

972-378-5554 | info@s3security.com
www.s3security.com

4975 Preston Park Blvd. Ste. 500
Plano, TX 75093

© 2025 Specialized Security Services, Inc. All Rights Reserved