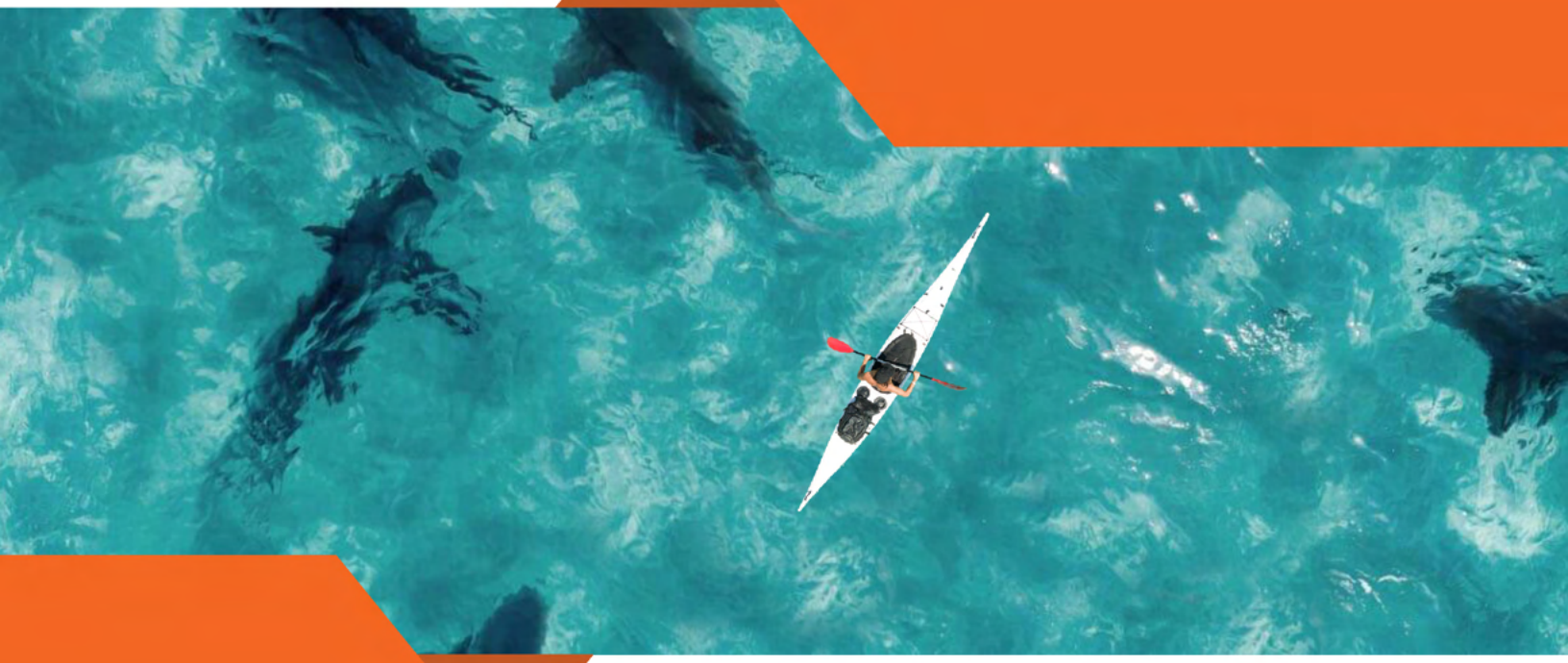

CYBERSECURITY SOLUTIONS FOR MANUFACTURERS

Protecting Production, Intellectual Property, & Business Continuity

SPECIALIZED S|3 SECURITY SERVICES

CYBERSECURITY IN MANUFACTURING

In manufacturing, uptime is everything. Whether you're producing aerospace components, consumer goods, or precision electronics, modern factories rely on smart technologies, digital supply chains, and interconnected systems. These innovations drive efficiency and scale, but they also introduce new cybersecurity risks that threaten operations, sensitive data, and brand reputation.

From legacy OT environments to third-party access and proprietary R&D, manufacturers must protect what matters most: production continuity, intellectual property, and regulatory compliance.

At S3 Security, we provide end-to-end support. We help you identify your top risks, align cybersecurity to business priorities, and deliver results from planning through execution.

© 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 go-to cybersecurity partner for businesses in high-risk, high-visibility industries. We go beyond offering solutions to build lasting relationships. As a full-service cybersecurity firm, we operate as an extension of your team. We help protect uptime, safeguard intellectual property, and secure supply chain operations. Our support also strengthens business continuity, profitability, and your reputation as a trusted supplier.

Whether you need help identifying risk, implementing solutions, or responding quickly to a threat, we deliver end-to-end support. Our services cover everything from assessments and remediation to project management and staff augmentation to ensure your initiatives succeed.

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

- ✓ **Founder-owned and independently operated –** We answer only to our clients, not investors.
- ✓ **One-stop cybersecurity partner –** From risk assessments and penetration testing to full remediation, staff augmentation, and ongoing project support, we cover it all.
- ✓ **Long-standing client relationships –** We support manufacturers in aerospace, automotive, medical devices, and consumer goods. Many have partnered with us for decades to protect operations, data, and long-term success.
- ✓ **Industry-leading expertise –** We understand the unique security challenges of manufacturing environments, including OT, IT, and regulatory compliance.
- ✓ **Custom-tailored security programs –** Our strategies are designed for your specific operations, not generic, one-size-fits-all frameworks.
- ✓ **Proactive, not reactive –** We detect and eliminate threats before they disrupt production or jeopardize safety.

Join the leading manufacturers that trust S3 Security to protect their operations, intellectual property, and reputation — and stay resilient today and into the future.

© 2025 Specialized Security Services, Inc. All Rights Reserved

KEY CYBERSECURITY CHALLENGES IN MANUFACTURING

Modern manufacturing is built on precision, automation, and connectivity, but with increased digitization comes increased cyber risk. From factory floors to global supply chains, protecting your systems and data is essential to maintaining uptime, safety, and competitive advantage.

Operational Technology (OT) Vulnerabilities

Legacy equipment and industrial control systems (ICS) often lack modern security controls. Weak segmentation, outdated firmware, and default credentials expose production environments to cyber threats.

Intellectual Property Theft

R&D data, proprietary designs, and trade secrets are prime targets for cyber espionage and insider threats, putting years of innovation and competitive edge at risk.

Compliance & Regulatory Pressure

Manufacturers must meet standards like NIST, CMMC, ITAR, and ISO 27001. Direct-to-consumer channels may also require PCI DSS compliance to protect payment data.

Ransomware & Downtime Attacks

Targeted ransomware can disrupt production lines, corrupt systems, and cause significant financial and operational loss.

Phishing & Social Engineering

Staff in finance, procurement, and operations are frequent phishing targets, putting sensitive systems and credentials at risk.

Cloud, ERP & IoT Security

Smart factories rely on connected systems that require strict access controls, well-defined security policies, and regular testing to identify vulnerabilities and prevent exploitation.

Global Footprint, Inconsistent Controls

Multi-site operations often face inconsistent security protocols due to regional regulations, outdated infrastructure, or decentralized oversight.

Third-Party & Supply Chain Risk

Suppliers and integrators introduce vulnerabilities. A single breach can compromise your entire ecosystem.

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

Staying compliant with cybersecurity and regulatory standards is essential for protecting intellectual property, maintaining operational continuity, meeting contractual requirements, and preserving customer trust.

- **NIST Cybersecurity Framework Assessments**
- **ISO 27001 Information Security Audits**
- **PCI DSS Assessments** (Payment Card Industry Data Security Standard) for direct to consumer
- **CMMC & ITAR Readiness & Assessments**
- **Cybersecurity Maturity Assessments for IT, OT, & Hybrid Environments**
- **Third-Party Vendor Risk Assessments**
- **Security Awareness Training for Staff**

BENEFIT

Strengthen compliance, safeguard business-critical data, and reduce the risk of costly disruptions across your operations.

© 2025 Specialized Security Services, Inc. All Rights Reserved

PENETRATION TESTING & VULNERABILITY MANAGEMENT

Identify and address security weaknesses before cybercriminals can disrupt operations or steal critical data.

- **Manufacturing Network & OT Penetration Testing**
- **Ransomware Simulation & Incident Response Testing**
- **Enterprise Application Security Testing**
- **Web Application & Infrastructure Vulnerability Scanning**
- **API & Cloud Security Assessments**
- **Wireless Network & Guest Wi-Fi Security Testing**
- **Third-Party Access & Remote Vendor Testing**
- **Dark Web & Open-Source Intelligence (OSINT) Monitoring**

BENEFIT

Reduce the risk of disruption, strengthen system integrity, and stay ahead of evolving cyber threats.

© 2025 Specialized Security Services, Inc. All Rights Reserved

DATA PROTECTION & PRIVACY

Data is more than an asset. In manufacturing, it's a competitive advantage. From product designs to customer insights and plant analytics, protecting sensitive information is essential to maintaining operational continuity, meeting regulatory demands, and enabling growth.

- **Intellectual Property & R&D Data Protection**
- **Enterprise Data Mapping & Governance**
- **Secure Supplier Data Sharing**
- **High-Value Access Oversight**
- **Information Lifecycle & Retention Strategy**
- **Insider Risk & Unstructured Data Controls**

BENEFIT

Protect innovation, minimize regulatory and operational risk, and gain visibility into the sensitive data that drives your business forward.

© 2025 Specialized Security Services, Inc. All Rights Reserved

INCIDENT RESPONSE & BUSINESS CONTINUITY

Limit operational disruption, financial loss, and safety risks in the event of a cyberattack or system failure.

- **Incident Response Planning & Tabletop Exercises**
- **Disaster Recovery & Ransomware Resilience Strategies**
- **Business Continuity Strategies & Operational Impact Testing**
- **Crisis Management & Communication Planning**

BENEFIT

Minimize downtime and financial loss while keeping production moving and stakeholders informed, even in the middle of a crisis.

© 2025 Specialized Security Services, Inc. All Rights Reserved

PROFESSIONAL CYBERSECURITY CONSULTING

Strategic guidance to strengthen your security posture, reduce risk across operations and partners, and ensure cybersecurity supports your business goals.

- **Virtual CISO (vCISO) Services**
- **Cybersecurity Staff Augmentation**
- **Cyber Risk Management & Governance**
- **Remediation Management & Assistance**
- **Security Policy & Procedure Development**
- **Secure Cloud ERP, & Industrial IoT Strategies**
- **Reputation & Contract Risk Protection**

BENEFIT

Gain top-tier cybersecurity expertise without the need for an in-house team.

© 2025 Specialized Security Services, Inc. All Rights Reserved

WHY MANUFACTURING LEADERS TRUST S3 SECURITY

Manufacturing-Focused Security

We understand the unique cybersecurity challenges in manufacturing, from protecting IP and OT systems to securing supply chains and production lines,

Proven Expertise

With over 25 years of experience securing high-risk, highly regulated industries, we understand the technical, regulatory, and operational challenges manufacturers face.

Custom-Tailored Programs

No off-the-shelf solutions; our cybersecurity strategies are designed to fit your workflows, environments, and compliance priorities.

Proactive Risk & Compliance Management

Stay ahead of threats while meeting CMMC, NIST, ISO, and ITAR requirements to reduce legal, operational, and contractual risk.

Resilient, Business-Centric Security

We focus on prevention, continuity, and long-term resilience, helping you avoid downtime and keep production moving securely.

Trusted by Industry Leaders

Global manufacturers rely on us for proven cybersecurity expertise and long-term partnerships that support resilience and growth.

PARTNER WITH S3 SECURITY TO PROTECT YOUR MANUFACTURING BUSINESS

TThe most successful manufacturers don't just react to cyber threats — they anticipate and prevent them. With S3 Security as your cybersecurity partner, you can protect your business, your IP, and your operations from digital risks without disrupting your supply chain or production goals.

Let us help you secure what drives your business today, and keep you prepared for what's next.

© 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 view of your cybersecurity posture, regulatory exposure, and operational risks. These first steps allow us to align with your business goals, prioritize risks, and build a roadmap for long-term protection.

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

- **Penetration Testing** – Internal, external, web application, OT systems, API, cloud and website testing to identify exploitable vulnerabilities before attackers do.
- **Vulnerability Assessment** – Internal and external scans to identify outdated software, system misconfigurations, and exposed services.
- **Enterprise Cybersecurity Gap Assessment** – A structured review against requirements like NIST, CMMC, ISO 27001, ITAR and PCI (when applicable) to assess compliance readiness and control maturity.
- **Enterprise Data Discovery** –dentification and classification of sensitive files, including design documents, engineering data, and supplier records that may be unencrypted or stored improperly.
- **Ransomware Simulation** – Test your ability to detect, contain, and recover from a simulated ransomware event, including impact on production and supply chain continuity.

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 collaborate closely with your team to build a tailored remediation strategy that reduces risk, improves security posture, and supports long-term operational resilience.

© 2025 Specialized Security Services, Inc. All Rights Reserved

ONGOING PROGRAM & STRATEGIC GUIDANCE

8 Weeks & Beyond:

After the initial phase, S3 Security will provide strategic recommendations for continued improvement. This may include:

- Ongoing remediation management and technical assistance
- Professional staff augmentation to support internal security & compliance efforts
- Implementation of long-term security services with recommended testing and review cadences

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 operational complexity of manufacturing and know that one of the greatest benefits of strong cybersecurity is uninterrupted performance and peace of mind.

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

With decades of experience guiding clients through changing regulatory requirements, emerging threats, and evolving infrastructure, we are your trusted partner in securing what drives your business.

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