SERKET-TECH SECURITY

Cybersecurity for Manufacturers: Protecting Production, IP, and Supply Chains

For manufacturers, plant operators, industrial suppliers, product companies, and manufacturing-adjacent service providers.

Manufacturing Cybersecurity is Business Continuity

Every plant now depends on connected systems such as ERP, MES, EDI, PLCs, industrial IoT, remote maintenance, cloud applications, supplier portals, and product engineering platforms. A cyber event can disrupt production, delay shipments, expose trade secrets, create contractual issues, and put safety and quality commitments under pressure.

Protect Production Uptime

Reduce the chance that ransomware, failed recovery, or remote access abuse disrupts plants, warehouses, engineering teams, or order fulfillment.

Secure Legacy OT and Industrial Systems

Improve visibility, segmentation, access control, and vulnerability handling across PLCs, HMIs, SCADA, CNC, robotics, sensors, and plant networks.

Meet Customer and Contract Demands

Prepare for supplier questionnaires, cyber insurance reviews, SOC 2, ISO 27001, CMMC, NIST 800-171, TISAX, PCI DSS, and other buyer-driven expectations.

Protect Intellectual Property

Safeguard CAD files, formulas, recipes, tooling data, product roadmaps, bills of material, test results, and controlled technical data.

Reduce Supply Chain Exposure

Review supplier access, remote vendors, managed service providers, plant contractors, EDI connections, and gray-market or counterfeit component risk.

Strengthen Response Readiness

Build plant-aware response plans, tabletop exercises, recovery workflows, and executive decision paths for downtime, extortion, data loss, or operational impact.

A Simple Delivery Model

Assess
Map sites, systems, contracts, and risks.

Prioritize
Rank gaps by production, safety, customer, and contract impact.

Implement
Build policies, controls, evidence, and workflows.

Validate
Test, tune, and prepare for customer or assessor review.

Operate
Monitor, improve, and sustain readiness year-round.

SERKET-TECH SECURITY

A Security Portfolio Built for Manufacturing

Services that connect governance, shop-floor risk, validation, and ongoing operations.

Full-Service Portfolio: Serket-Tech Security helps manufacturing organizations mature without turning security into a production blocker.

Governance, Risk, and Compliance

Risk assessments, policy programs, control mapping, board and executive reporting, cyber insurance support, and customer audit preparation.

CMMC and Defense Supplier Readiness

NIST 800-171 gap reviews, SPRS score support, CUI scoping, SSP and POA&M development, CMMC readiness, and assessor preparation.

Supply Chain And Vendor Risk

Supplier security reviews, remote vendor access controls, managed service provider oversight, EDI and integration review, and stronger inherited-control documentation.

Managed Security Services

Threat monitoring, endpoint protection, MDR support, alert triage, vulnerability management, evidence tracking, and continuous control monitoring.

Penetration Testing

External, internal, cloud, wireless, web application, and remote access testing with prioritized findings and remediation guidance.

OT and Industrial Control Security

OT asset visibility, network segmentation, secure remote access, vulnerability handling, backup strategy, and plant-aware control design.

Security Assessments and Remediation

Cloud, ERP, MES, EDI, identity, endpoint, email, network, and architecture reviews with practical remediation planning.

Incident Response And Resilience

Ransomware playbooks, plant downtime exercises, breach support, forensics coordination, crisis communications, and backup and recovery validation.

Data, IP, And Product Security

Access governance, DLP planning, engineering data protection, secure collaboration, export-controlled data workflows, and product lifecycle system review.

Executive Advisory And Future Risk

vCISO support, AI governance, secure adoption of automation tools, cryptographic risk review, and post-quantum planning.

Frameworks and Requirements We Can Support

- **Core Security**
  NIST CSF 2.0, CISA CPGs, ISO 27001, SOC 2, PCI DSS, cyber insurance control sets
- **Automotive and Mobility Suppliers**
  TISAX readiness, ISO 27001 alignment, supplier security questionnaires, prototype and product data protection
- **OT and Plant Environments**
  NIST SP 800-82, ISA/IEC 62443, Purdue model segmentation, secure remote access, plant incident response
- **Medical Device and Life Sciences**
  FDA medical device cybersecurity, 21 CFR Part 11 support, HITRUST path support when customers require healthcare assurance
- **Defense and Aerospace Suppliers**
  CMMC, NIST SP 800-171, DFARS, FCI, and CUI handling, ITAR, and EAR data protection workflows
- **Global And Customer-Driven Needs**
  Privacy requirements, customer audits, supplier codes of conduct, third-party assurance, and executive reporting

SERKET-TECH SECURITY

How Manufacturing Clients Engage Serket-Tech Security

Start with the highest pressure area, then expand into a repeatable operating model.

1. Plant Cyber Baseline and Roadmap

For manufacturers that need a clear view of exposure across IT, OT, cloud, plants, and remote access.

What We Deliver

- IT and OT discovery interviews
- Production-impact risk review
- Network, identity, endpoint, and remote access analysis
- Prioritized remediation plan
- Executive roadmap for budget and ownership

2. Contract, Customer, and Assurance Readiness

For suppliers facing questionnaires, customer audits, defense contracts, automotive requirements, or regulated product obligations.

What We Deliver

- CMMC and NIST 800-171 readiness
- SOC 2, ISO 27001, PCI DSS, HITRUST, or TISAX path support
- SSP, POA&M, policy, and evidence development
- Customer questionnaire response support
- Assessor and audit coordination

3. Continuous Security Operations and Resilience

For organizations that want security readiness to become part of daily operations across plants and business systems.

What We Deliver

- MDR and endpoint protection support
- Vulnerability management and patch prioritization
- Control monitoring and evidence collection
- Incident response planning and tabletop exercises
- Recurring executive reporting and improvement cycles
- Executive reporting and improvement tracking

Manufacturing Pain Points this Brochure is Designed to Address

→ Downtime Economics
Lost production, missed shipments, overtime, scrap, warranty exposure, and customer penalties can outweigh the visible IT recovery cost.

→ Legacy and Unsupported Systems
Manufacturing environments often carry long-lived equipment, flat networks, shared accounts, outdated software, and limited maintenance windows.

→ Customer Trust Pressure
Large customers now expect suppliers to prove security maturity through questionnaires, audits, certifications, and contractual controls.

→ Sensitive Product Information
Engineering drawings, prototypes, pricing, recipes, formulas, process settings, and controlled technical data need stronger access and sharing rules.

→ IT and OT Ownership Gaps
Plant engineering, IT, maintenance, vendors, and business leadership often share risk without a shared operating model.

→ Remote Access and Vendor Dependency
OEMs, integrators, contractors, and support providers need access, but that access must be governed, monitored, and limited.

→ Business Email and Payment Fraud
Quote changes, invoice redirection, supplier impersonation, and purchase order fraud can occur during normal business operations.

→ Mergers, New Sites, and Digital Modernization
Acquisitions, new plants, cloud migrations, robotics, and Industry 4.0 programs can create hidden cyber and compliance gaps.

SERKET-TECH SECURITY

Why Serket-Tech Security

A practical partner for manufacturers that need action, validation, and sustained readiness.

Who We Serve

- Discrete and process manufacturers
- Industrial equipment and machinery companies
- Aerospace and defense suppliers
- Automotive and mobility suppliers
- Electronics, semiconductor, and component manufacturers
- Food, beverage, chemical, and packaging companies
- Medical device, pharma, and life sciences manufacturers
- Contract manufacturers and manufacturing service providers

Why The Model Works

- One partner across strategy, remediation, testing, and operations
- Delivery that respects production schedules and plant constraints
- Coverage for IT, OT, cloud, identity, endpoint, and supplier access
- Support for assurance, contracts, cyber insurance, and customer diligence
- Practical roadmaps that leaders can fund and teams can execute
- Continuity from readiness work into managed operations

A Broad Security and Compliance Portfolio

Identity And Access
MFA, privileged access, shared account reduction, remote vendor controls, and lifecycle reviews.

Executive Reporting
Risk, control maturity, budget priorities, incident readiness, and program progress in business language.

Backup And Recovery
Recovery point review, isolation, restore testing, and ransomware response planning.

Detection And Response
Endpoint, email, network, cloud, and identity monitoring tied to usable response playbooks.

Evidence And Audit Readiness
Policies, procedures, control owners, recurring evidence, and customer-ready documentation.

Segmentation And Visibility
IT and OT boundary review, asset discovery, traffic paths, and safer plant connectivity.

Build A Manufacturing Security Program That Is Production-Aware, Customer-Ready, And Contract-Ready

Engage Serket-Tech Security for a readiness workshop, plant cyber baseline, CMMC readiness review, OT security assessment, tabletop exercise, penetration test, or managed security program design.