TACJE

TRANSNATIONAL ACADEMIC JOURNAL OF ECONOMICS

Transnational Academic Journal of Economics, Year: 2026, Volume: 3, Issue: 1, Pages : 1-14 *Research Article*

DOI: 10.5281/zenodo.18421438

Publication Date: 30.01.2026

Oleksandr Khodorkovskyi[1]

1. *ORCID: https://orcid.org/0009-0007-4242-3625 Email: olexandr.c86@yahoo.com Quantum Core, Ukraine*

Cybersecurity of SaaS Products Threats, Secure-by-Design Engineering, and Security Metrics for Continuous Assurance

Abstract

Software-as-a-Service (SaaS) concentrates business-critical data and identity workflows into always-on, internet-exposed systems, making it a prime target for credential theft, API abuse, supply-chain compromise, and cloud-control-plane attacks. This paper develops a secure-by-design framework for SaaS that integrates (i) governance and risk outcomes from NIST CSF 2.0, (ii) security and privacy controls from NIST SP 800-53 Rev. 5 and ISO/IEC 27001, and (iii) secure software engineering practices from NIST SP 800-218 (SSDF), combined with application-layer standards such as OWASP ASVS and OWASP API Security Top 10 (2023). OWASP Foundation+5NIST Computer Security Resource Center+5NIST Computer Security Resource Center+5 Results include a reference architecture for secure SaaS delivery (Figure 1) and a metrics-based control matrix (Table 1) linking threat categories to measurable security outcomes, aligned with SOC 2 Trust Services Criteria and cloud assurance mapping via CSA CCM. AICPA & CIMA+2Cloud Security Alliance+2 The paper concludes that resilient SaaS security requires unifying secure development, identity-centric architecture, supply-chain integrity (SBOM/SLSA), and operational telemetry into a continuous assurance loop.

Keywords: SaaS security; secure-by-design; zero trust; API security; SSDF; SOC 2; security metrics; supply chain security

How to cite: Khodorkovskyi O. Cybersecurity of SaaS Products Threats, Secure-by-Design Engineering, and Security Metrics for Continuous Assurance. *Transnational Academic Journal of Economics, 3*(1), 1-14

Introduction

SaaS has become a default delivery model for enterprise applications, driven by rapid deployment, elastic scaling, and subscription economics. Yet the same characteristics that create business value—multi-tenancy, extensive integrations, identity federation, and continuous delivery—expand attack surfaces and amplify blast radius. A single SaaS compromise can expose large volumes of customer data, create privileged access pathways to downstream systems, and disrupt business processes for thousands of tenants simultaneously.SaaS cybersecurity differs from traditional on-premises security in several ways. First, the control boundary shifts: customers depend on the provider for platform hardening, secure development, patching, and incident response, while retaining responsibility for their own identity governance, configuration, and access management. Second, SaaS systems are typically built around API-first architectures and integrated ecosystems, where third-party connections and automation pipelines are central to functionality but also create systemic security dependencies. The OWASP API Security Top 10 (2023) underscores that authorization, authentication, and inventory failures are persistent high-impact API risks, and these map directly onto common SaaS breach patterns. OWASP Foundation+1 Third, SaaS delivery pipelines are inseparable from software supply chains: build systems, dependencies, containers, and infrastructure-as-code become security-critical assets.The secure-by-design paradigm aims to address these realities by moving security from reactive controls to product engineering fundamentals. The CISA Secure by Design Pledge reflects an industry-wide push to raise the baseline of software security by embedding practices such as stronger authentication, reduced default insecurity, and improved vulnerability handling into products. CISA+1 While voluntary, the pledge signals a direction of travel: shifting responsibility from end users to vendors, increasing transparency, and adopting measurable security improvements.A rigorous SaaS security program requires (i) governance and risk framing, (ii) secure software engineering, and (iii) operational security telemetry that enables continuous assurance. NIST CSF 2.0 provides a widely applicable taxonomy of cybersecurity outcomes and strengthens governance alignment as a first-order element of cybersecurity management. NIST Computer Security Resource Center+2NIST Publications+2 At the control level, NIST SP 800-53 Rev. 5 provides a comprehensive catalog of security and privacy controls spanning access control, audit/accountability, incident response, configuration management, system integrity, and supply chain risk management. NIST Computer Security Resource Center+1 ISO/IEC 27001:2022 similarly establishes requirements for an information security management system (ISMS) with continual improvement, and is often used by SaaS providers as a certification-oriented governance mechanism. ISO+1.Secure-by-design also requires embedding security into the software development lifecycle. NIST SP 800-218 (SSDF) formalizes a core set of secure development practices that can be integrated into SDLC processes and used as a common vocabulary across producers and consumers. NIST Computer Security Resource Center+1 OWASP ASVS provides a practical verification standard for web applications and services, supporting structured security requirements, testing, and assurance across maturity levels. OWASP Foundation+1.For SaaS, architecture-level paradigms must reflect modern threat realities. NIST SP 800-207 defines Zero Trust Architecture (ZTA) as a shift from implicit trust based on network location to resource-centric access decisions based on identity and context—highly relevant in SaaS ecosystems with remote users, cloud assets, and federated identity. NIST Computer Security Resource Center+1 Threat modeling should also incorporate cloud-specific adversary behaviors, where control-plane compromise, identity provider attacks, and SaaS-to-SaaS lateral movement are increasingly prominent; the MITRE ATT&CK Cloud Matrix provides a structured mapping of tactics and techniques across SaaS, IaaS, identity providers, and office suites. MITRE ATT&CK+1.Finally, SaaS cybersecurity must be measurable. Customers, regulators, and

boards demand evidence of security effectiveness, not only security intent. SOC 2 examinations provide independent reporting on controls relevant to security, availability, processing integrity, confidentiality, and privacy. AICPA & CIMA+1 Cloud assurance mapping can be strengthened via the Cloud Security Alliance Cloud Controls Matrix (CCM), which enumerates control objectives and clarifies shared responsibility across cloud supply chains. Cloud Security Alliance+1

Research objectives

This paper aims to:

Define a reference secure-by-design architecture for SaaS products (Figure 1) grounded in NIST CSF 2.0, Zero Trust, and SSDF practices. NIST Computer Security Resource Center+2NIST Computer Security Resource Center+2

Establish a threat-and-controls model for SaaS that includes API security and cloud threat techniques, mapped to standardized control frameworks. OWASP Foundation+1

Propose measurable security metrics that support continuous assurance and customer-facing evidence (Table 1), aligned to SOC 2 and CSA CCM. AICPA & CIMA+1

Integrate software supply chain protections (SBOM/SLSA; C-SCRM) into SaaS security engineering and operations. NTIA+2SLSA+2

Materials and Methods

Materials (standards, frameworks, and authoritative sources)

Governance and controls frameworks

NIST CSF 2.0, including its outcomes-driven taxonomy and governance emphasis. NIST Computer Security Resource Center+2NIST Publications+2

NIST SP 800-53 Rev. 5 control catalog for security and privacy controls. NIST Computer Security Resource Center+1

ISO/IEC 27001:2022 requirements for an ISMS. ISO+1

CIS Critical Security Controls v8 (prioritized best practices) for pragmatic implementation sequencing. CIS+1

CSA Cloud Controls Matrix v4 (cloud control objectives and shared responsibility). Cloud Security Alliance+1

SOC 2 Trust Services Criteria overview and guidance for service organizations. AICPA & CIMA+1

Secure engineering and application/API security standards

NIST SP 800-218 (SSDF) secure software development practices for SDLC integration and supplier communications. NIST Computer Security Resource Center+1

NIST SP 800-207 Zero Trust Architecture for identity- and context-centric access decisions. NIST Computer Security Resource Center+1

OWASP Top 10 (2021) and OWASP API Security Top 10 (2023) for web and API risk baselines. OWASP Foundation+1

OWASP ASVS for verification requirements for web services and applications. OWASP Foundation+1

Supply chain integrity and transparency

NIST SP 800-161r1 (Cybersecurity Supply Chain Risk Management) for integrating C-SCRM into enterprise risk and procurement. NIST Computer Security Resource Center+1

NTIA "Minimum Elements for a Software Bill of Materials (SBOM)" and associated public notice context. NTIA+1

SLSA framework for supply-chain levels and artifact integrity controls. SLSA+1

Threat modeling references

MITRE ATT&CK Cloud Matrix for SaaS and cloud attack techniques and coverage planning. MITRE ATT&CK

Methods (analytic approach)

Step 1: SaaS threat taxonomy construction.

We constructed a threat taxonomy organized by SaaS architecture layers: identity and access, API surface, application logic, data layer, infrastructure/control plane, CI/CD and dependencies, and operational processes. Threat categories were informed by OWASP Top 10 (2021), OWASP API Top 10 (2023), and ATT&CK Cloud tactics. OWASP Foundation+2OWASP Foundation+2

Step 2: Control mapping.

Controls were mapped to NIST SP 800-53 Rev. 5 families (e.g., Access Control, Audit and Accountability, Incident Response, Configuration Management, System and Information Integrity, Supply Chain Risk Management) and to ISO/IEC 27001:2022 ISMS processes. NIST Computer Security Resource Center+1

Step 3: Secure-by-design synthesis.

SSDF practices were mapped to SDLC phases (requirements, design, implementation, verification, release, and maintenance). This mapping provides a repeatable mechanism for integrating secure engineering with governance and assurance expectations. NIST Computer Security Resource Center+1

Step 4: Metrics model.

We designed a metrics framework with three tiers:

- **Leading indicators** (process and control coverage, e.g., MFA adoption, SBOM coverage).
- **Operational indicators** (detection and response, e.g., mean time to detect/contain).

Outcome indicators (impact, e.g., breach frequency/severity, availability SLO attainment). Metrics were aligned to CSF 2.0 outcomes and SOC 2 assurance themes, with cloud control mapping to CSA CCM. NIST Computer Security Resource Center+2AICPA & CIMA+2

Step 5: Artifacts.

Two artifacts summarize the synthesis: Figure 1 (architecture) and Table 1 (controls and metrics matrix).

Results

Main result: SaaS security is an identity- and supply-chain-centered control system

The primary result is that high-confidence SaaS cybersecurity emerges from the combination of:

identity-centric architecture (Zero Trust), NIST Computer Security Resource Center

secure software development (SSDF + verification standards), NIST Computer Security Resource Center+1

cloud assurance and shared responsibility mapping (CSA CCM), Cloud Security Alliance+1

supply chain integrity and transparency (SBOM/SLSA + C-SCRM), NTIA+2SLSA+2 and

measurable operational outcomes anchored in governance frameworks (NIST CSF 2.0, SOC 2). NIST Computer Security Resource Center+1

Figure 1 (mandatory figure)

Figure 1. Reference secure-by-design architecture for SaaS (engineering → operations → assurance loop)

(1) Governance & Risk (CSF 2.0 / ISO 27001 / SOC 2)

- risk appetite, policies, secure-by-design objectives
- control ownership, audit evidence plan, shared responsibility mapping (CCM)

▼

(2) Identity-Centric Access (Zero Trust)

- SSO/OIDC/SAML, MFA, conditional access, device posture
- least privilege, just-in-time admin, secrets management

▼

(3) SaaS Application & API Layer (OWASP Top 10 + API Top 10 / ASVS)

- robust authorization (object- and function-level)
- rate limiting, abuse prevention, secure session management
- secure multi-tenant isolation and per-tenant encryption

(4) Data & Key Management

- encryption in transit and at rest; key rotation
- data lifecycle controls, retention, deletion, backups, restore testing

(5) CI/CD & Supply Chain Integrity (SSDF + SBOM + SLSA + C-SCRM)

- secure build, signed artifacts, dependency governance
- SBOM publication, provenance attestations, supplier risk controls

(6) Security Operations (Telemetry & Response)

- centralized logging, detection engineering, incident response
- vulnerability management, patch SLAs, configuration drift control

(7) Continuous Assurance & Customer Evidence

- metrics dashboards (Table 1), control testing, SOC 2 reporting cadence
- improvement actions feed back to governance and engineering

Figure 1 aligns outcome governance from NIST CSF 2.0 with secure engineering (SSDF) and cloud assurance mapping (CSA CCM), while reflecting Zero Trust principles for SaaS access decisions. NIST Computer Security Resource Center+3NIST Computer Security Resource Center+3NIST Computer Security Resource Center+3

Table 1 (mandatory table)

Table 1. SaaS threat categories, secure-by-design controls, and measurable security metrics

Threat category	Representative attack patterns	Secure-by-design controls (examples)	Evidence artifacts	Metrics (examples)
Identity compromise	credential stuffing, session hijack, IdP misuse	MFA + conditional access; least privilege; ZTA; admin JIT NIST Computer Security Resource Center+1	access logs; IAM policies; admin review records	MFA adoption rate; privileged access anomalies; % JIT usage
API abuse	broken object-level auth; inventory gaps	authorization-by-default; API inventory; schema validation; rate limits OWASP Foundation+1	API gateway config; test reports	BOLA findings rate; API endpoint coverage; abuse blocks/day
App-layer vulnerabilities	injection, misconfig, SSRF	ASVS-based verification; secure code review; WAF; secure defaults OWASP Foundation+1	SAST/DAST results; pentest reports	critical vulns open>30d; fix SLA attainment
Multi-tenant isolation failure	cross-tenant data access	tenant-aware authorization; partitioned storage; per-tenant keys	architecture docs; access tests	cross-tenant test pass rate; isolation regressions/release
Cloud control-plane compromise	IAM role abuse, misconfigured cloud resources	CSA CCM mapping; config-as-code; drift detection Cloud Security Alliance+1	cloud posture reports; IaC baselines	config drift MTTR; % resources compliant
Supply chain attack	dependency poisoning; build tampering	SSDF practices; signed builds; SBOM; SLSA provenance NIST Computer Security Resource Center+2NTIA+2	SBOM records; provenance attestations	% releases with SBOM; provenance coverage; unsigned artifact rate
Detection/response gaps	insufficient logging; slow containment	centralized logs; IR playbooks; SOC 2-aligned evidence NIST Computer Security Resource Center+1	IR runbooks; detection rules	MTTD/MTTR; alert fidelity; incident recurrence rate
Availability/Resilience	DoS, dependency outages	resilience testing; backup/restore drills; SLOs	DR test reports; SLO dashboards	availability %; RTO/RPO achieved; failed restores

Table 1 anchors controls in widely used standards and frameworks (OWASP, NIST, CSA CCM, SSDF, SBOM/SLSA, SOC 2) and expresses them as measurable indicators suitable for continuous assurance. AICPA & CIMA+5OWASP Foundation+5NIST Computer Security Resource Center+5

3.1 Threat landscape and control priorities for SaaS

The SaaS threat landscape is dominated by identity compromise, API exposure, and misconfiguration—patterns reinforced by application and API security risk baselines. The OWASP Top 10 (2021) highlights recurring web risks (e.g., broken access control and security misconfiguration) that remain highly relevant to SaaS multi-tenant environments. OWASP Foundation+1 The OWASP API Security Top 10 (2023) further emphasizes broken object-level authorization and improper inventory management as critical API risks; these align closely with SaaS breach narratives where attackers enumerate tenant objects or abuse undocumented endpoints. OWASP Foundation+1.Cloud-native threats broaden this landscape. The MITRE ATT&CK Cloud Matrix provides a structured model for cloud tactics and techniques across SaaS, identity providers, and IaaS, enabling security teams to reason about adversary behaviors that traverse identity, applications, and management planes. MITRE ATT&CK+1 For SaaS providers, a practical implication is that high-impact threats often exploit weak identity governance (privileged roles, weak MFA, token theft) and the security externalities created by integrations and automation.

Consequently, control priorities should be sequenced:

identity hardening and zero-trust decisioning, NIST Computer Security Resource Center

API authorization-by-default and inventory governance, OWASP Foundation

secure-by-design SDLC and verification (ASVS), OWASP Foundation+1

cloud configuration governance with mapped controls (CSA CCM), Cloud Security Alliance+1 and

detection and response maturity to reduce dwell time and recurrence.

3.1.1 Supply-chain integrity as a first-class SaaS security requirement

SaaS security depends on the integrity of its software supply chain: dependencies, build systems, CI/CD automation, container images, and deployment infrastructure. NIST SP 800-218 (SSDF) provides a core set of secure software development practices that can be integrated into SDLC models and used as a shared vocabulary between producers and consumers. NIST Computer Security Resource Center+1 SSDF is complementary to NIST's broader supply-chain guidance in SP 800-161r1, which integrates cybersecurity supply chain risk management (C-SCRM) into enterprise risk management and acquisition processes. NIST Computer Security Resource Center+1. Transparency and provenance further strengthen SaaS assurance. NTIA's "Minimum Elements for a Software Bill of Materials (SBOM)" defines SBOM as a formal record containing details and supply chain relationships of components used to build software, supporting vulnerability response and supplier transparency. NTIA+1 SLSA provides incrementally adoptable levels and controls to prevent tampering and improve artifact integrity, establishing a shared language for strengthening supply chains "from source to service." SLSA+1

For SaaS providers, these elements imply implementable design requirements:

generate SBOMs for every release and integrate SBOM consumption into vulnerability management workflows; NTIA

enforce signed builds and provenance attestations for deployment artifacts (SLSA-aligned); SLSA

apply supplier risk evaluation and dependency governance (C-SCRM); NIST Computer Security Resource Center

audit build pipelines as production-critical assets, because build compromise is functionally equivalent to production compromise.

Numbered lists can be added as follows

Define shared responsibility explicitly: map SaaS controls to CSA CCM domains and publish customer guidance for identity, configuration, and logging integration. Cloud Security Alliance+1

Implement Zero Trust access decisions: enforce MFA, conditional access, and least privilege; remove implicit trust based on network location. NIST Computer Security Resource Center+1

Adopt "authorization-by-default" for APIs: treat BOLA and endpoint inventory as non-negotiable engineering requirements (OWASP API Top 10 2023). OWASP Foundation

Institutionalize secure development practices: integrate SSDF practices into SDLC and procurement communications; use ASVS to verify implementation. NIST Computer Security Resource Center+1

Treat CI/CD as production: implement SBOM generation, provenance, and signed artifacts; align controls to SLSA levels. NTIA+1

Measure continuously: adopt metrics from Table 1 with thresholds; align reporting to CSF 2.0 outcomes and SOC 2 trust criteria. NIST Computer Security Resource Center+1

Close the loop: use incident learnings and detection outcomes to update engineering requirements and verification tests (continuous assurance).

Discussion

Secure-by-design as a convergence of governance, engineering, and operations

The results show that SaaS security cannot be achieved by operational monitoring alone or by SDLC practices alone. Rather, secure-by-design requires convergence: governance defines risk tolerances and accountability, engineering prevents classes of vulnerabilities, and operations detects and contains residual risk. NIST CSF 2.0 is useful because it provides an outcomes-based model that supports communication across boards, security teams, and engineering organizations, and positions governance as central rather than peripheral. NIST Computer Security Resource Center+1.NIST SP 800-53 Rev. 5 adds implementable control breadth, while ISO/IEC 27001:2022 provides an ISMS mechanism for continual improvement and certification-driven assurance. NIST Computer Security Resource Center+1 In SaaS markets, these are frequently paired with SOC 2 reports as customer-facing evidence of control design and operating effectiveness. SOC 2's trust criteria framing aligns naturally to SaaS concerns: security (baseline), availability (service continuity), confidentiality and privacy (data governance), and processing integrity (correct system behavior). AICPA & CIMA+1

Identity and APIs: the dominant SaaS risk multipliers

Identity and APIs are the primary risk multipliers in SaaS. Zero Trust Architecture (NIST SP 800-207) is particularly relevant because SaaS is inherently perimeterless: users are remote, resources are distributed, and integrations are constant. NIST Computer Security Resource Center+1 The OWASP API Top 10 (2023) demonstrates that broken authorization and poor inventory management remain severe and common, and SaaS providers often unintentionally amplify these risks through rapid feature delivery and partner integrations. OWASP Foundation+1 Therefore, secure-by-design implies "API governance by construction": inventory, authentication, authorization, rate limiting, and schema enforcement are not optional add-ons but base product architecture.

Supply chain: the systemic risk channel

Modern SaaS security failures often originate upstream: dependencies and build pipelines. NIST SP 800-161r1 (C-SCRM) provides structured guidance for integrating supply-chain risk into enterprise risk management and planning. NIST Computer Security Resource Center+1 SSDF provides secure development practices, but SaaS providers also need transparency artifacts such as SBOMs and provenance. NTIA's minimum elements for SBOM establish a baseline for what SBOMs should contain and why they matter. NTIA+1 SLSA extends this into integrity controls and maturity levels that can be adopted incrementally. SLSA+1.A practical insight is that SBOM and provenance only become security-relevant when integrated into operations: vulnerability management must consume SBOMs; deployment pipelines must verify signatures; procurement must require supplier disclosures; and incident response must include supply-chain hypotheses.

Metrics and continuous assurance

SaaS security programs frequently fail due to poor measurability: teams track activity (tickets closed) rather than outcomes (risk reduced). The metrics model proposed here emphasizes leading indicators (e.g., MFA adoption, SBOM coverage), operational indicators (MTTD/MTTR), and outcome indicators (availability SLOs, incident recurrence). This is compatible with the outcomes focus of CSF 2.0 and with SOC 2's control-operating-effectiveness expectations. NIST Computer Security Resource Center+1 Mapping via CSA CCM also helps clarify which controls are provider responsibilities versus customer responsibilities, improving both assurance and adoption. Cloud Security Alliance+1

Industry direction: secure-by-design pledge signals

The CISA Secure by Design Pledge signals a normative shift toward measurable, vendor-owned security improvements. CISA+1 For SaaS providers, the strategic implication is that security maturity will increasingly be evaluated not only by certifications but by evidence of secure defaults and demonstrable reductions in systemic risk.

Conclusions

SaaS cybersecurity is a high-exposure, high-consequence discipline shaped by identity-centric architectures, API-first design, and continuous delivery. The core conclusion of this paper is that secure-by-design for SaaS must be implemented as a continuous assurance loop linking governance, secure engineering, and operational telemetry.NIST CSF 2.0 provides an outcomes-driven governance backbone that helps align executive accountability, risk management, and security investment. NIST Computer Security Resource Center+1 NIST SP 800-53 Rev. 5 and ISO/IEC 27001:2022 provide the control and management-system foundations necessary to demonstrate repeatable processes and auditability. NIST Computer Security Resource Center+1 NIST SP 800-218 (SSDF) and OWASP verification standards translate these governance expectations into secure development practices and testable requirements, reducing vulnerability injection and improving release confidence. NIST Computer Security Resource Center+1.At the architecture layer, Zero Trust principles are essential because SaaS dissolves traditional network perimeters; access decisions must be identity- and context-driven, with least privilege and strong authentication as defaults. NIST Computer Security Resource Center+1 At the interface layer, the OWASP API Top 10 (2023) demonstrates that broken authorization and unmanaged API inventory are persistent risks that demand "governance by construction." OWASP Foundation At the ecosystem layer, the MITRE ATT&CK Cloud Matrix underscores that attackers exploit identity providers and cloud control planes to achieve lateral movement and persistent access, motivating cloud-threat-informed detection coverage planning. MITRE ATT&CK.Supply chain security is inseparable from SaaS security. C-SCRM guidance (NIST SP 800-161r1), SBOM minimum elements (NTIA), and SLSA integrity controls should be treated as baseline requirements to prevent and quickly respond to dependency and build compromise. NIST Computer Security Resource Center+2NTIA+2 The practical success condition is integration into operations: SBOMs must be consumed by vulnerability management; provenance must be enforced at deployment; and supplier risk must influence procurement and engineering.Finally, security metrics must move from narrative to measurement. The metrics and control matrix proposed in Table 1 provides a structured way to demonstrate security effectiveness to customers and auditors, aligning to SOC 2 trust criteria and cloud assurance mapping via CSA CCM. AICPA & CIMA+1 Providers that unify these elements—governance, secure engineering, supply chain integrity, and measurable operations—will achieve more resilient SaaS security and stronger customer trust in an environment where security expectations are steadily becoming more explicit and evidence-driven.

Patents

No patents are claimed. Potential patentable contributions could include: (i) automated multi-tenant isolation verification tools that continuously test cross-tenant access pathways; (ii) continuous assurance scoring models that combine SBOM/provenance, identity posture, and runtime telemetry into a single risk metric; (iii) cryptographic audit trails binding deployment provenance, configuration states, and customer-impacting security decisions; and (iv) privacy-preserving anomaly detection for SaaS audit logs to identify abuse patterns without exposing tenant-sensitive content.

Supplementary Materials

Supplementary materials may include: (i) a SaaS security controls mapping worksheet (CSF 2.0 → 800-53 → ISO 27001 → SOC 2 → CSA CCM); (ii) an API inventory and authorization verification checklist aligned to OWASP API Top 10 (2023); (iii) SBOM and SLSA provenance templates; (iv) a CI/CD hardening playbook aligned to SSDF; and (v) a metrics dashboard specification implementing the KPIs listed in Table 1.

Author Contributions

Conceptualization: O. Khodorkovskyi. Methodology: O. Khodorkovskyi. Formal analysis: O. Khodorkovskyi. Investigation: O. Khodorkovskyi. Writing—original draft: O. Khodorkovskyi. Writing—review and editing: O. Khodorkovskyi. Visualization (Figure 1; Table 1): O. Khodorkovskyi. Supervision: Not applicable. Project administration: Not applicable.

Funding

No external funding was received. Future empirical validation using real SaaS incident datasets, security telemetry, and customer assurance data may require funding to support secure data enclaves, red-teaming exercises, and independent audits.

Institutional Review Board Statement

Not applicable. This study synthesizes publicly available standards, frameworks, and guidance documents. No human participants were recruited, and no personal data were collected. Any future research involving user studies, SOC analyst workflow assessments, or customer-impact analysis should follow appropriate ethics review processes and data protection regulations.

Informed Consent Statement

Not applicable. No human subjects were involved. Future studies that include surveys or interviews with security engineers, SOC analysts, or customers should obtain informed consent and ensure confidentiality for sensitive operational information.

Acknowledgments

The author acknowledges the organizations that provide widely adopted cybersecurity and secure engineering guidance for SaaS providers, including NIST (CSF 2.0, SP 800-53, SSDF, Zero Trust, C-SCRM), OWASP (ASVS and API Security Top 10), the Cloud Security Alliance (CCM), and NTIA and OpenSSF communities advancing SBOM and SLSA practices for supply-chain integrity. SLSA+7NIST Computer Security Resource Center+7NIST Computer Security Resource Center+7

Conflicts of Interest

The author declares no conflicts of interest. The author has no financial or personal relationships with vendors of cloud security, SIEM, vulnerability management, or compliance automation platforms that could be perceived as influencing the analysis.

Appendix A

Minimum viable secure-by-design requirements for SaaS releases

A1. Identity baseline: MFA enforced for privileged roles; least privilege; JIT admin. NIST Computer Security Resource Center+1

A2. API baseline: endpoint inventory; object- and function-level authorization checks; rate limits. OWASP Foundation

A3. SDLC baseline: SSDF practices integrated; ASVS verification for critical flows. NIST Computer Security Resource Center+1

A4. Supply chain baseline: SBOM per release; signed artifacts; provenance checks (SLSA-aligned). NTIA+1

A5. Logging baseline: centralized audit logs; retention; alerting on high-risk events (800-53). NIST Computer Security Resource Center+1

A6. Resilience baseline: backup/restore tested; availability SLO reporting.

Appendix B

Metrics governance protocol (continuous assurance)

B1. Define metric owners and thresholds; align outcomes to CSF 2.0 categories. NIST Computer Security Resource Center+1

B2. Maintain evidence artifacts for audits (SOC 2) and customer reporting. AICPA & CIMA+1

B3. Track leading indicators monthly (MFA adoption, SBOM coverage, critical vuln SLA). NTIA+1

B4. Track operational indicators continuously (MTTD/MTTR, drift in alert quality).

B5. Review incidents quarterly and update engineering requirements accordingly (SSDF feedback loop). NIST Computer Security Resource Center+1

B6. Map customer responsibilities using CSA CCM and communicate configuration expectations. Cloud Security Alliance+1

References

1. NIST. *CSWP 29: The NIST Cybersecurity Framework (CSF) 2.0 (Final).* NIST Computer Security Resource Center+1
2. NIST. *Cybersecurity Framework (CSF) program page and updates.* NIST
3. NIST. *SP 800-53 Rev. 5 (Update 1): Security and Privacy Controls for Information Systems and Organizations.* NIST Computer Security Resource Center
4. ISO. *ISO/IEC 27001:2022 — Information security management systems — Requirements (standard overview page).* ISO
5. ISO/IEC. *ISO/IEC 27001:2022 (publicly accessible PDF copy).* eiso.upm.edu.my

6. NIST. *SP 800-218: Secure Software Development Framework (SSDF) v1.1 (Final).* NIST Computer Security Resource Center
7. CISA. *NIST SP 800-218 SSDF resource page.* CISA
8. NIST. *SP 800-207: Zero Trust Architecture (Final).* NIST Computer Security Resource Center+1
9. OWASP. *Application Security Verification Standard (ASVS) project page.* OWASP Foundation
10. OWASP. *ASVS GitHub repository (v4 series artifacts).* GitHub+1
11. OWASP. *OWASP Top Ten 2021 (official materials).* GitHub+1
12. OWASP. *OWASP Top 10 release notes and process (2021 cycle).* owasptopten.org
13. OWASP. *OWASP API Security Top 10 – 2023 (official list).* OWASP Foundation
14. CSA. *Cloud Controls Matrix (CCM) research page.* Cloud Security Alliance
15. CSA. *Cloud Controls Matrix and CAIQ v4 (release and download artifact page).* CSA+1
16. AICPA & CIMA. *SOC 2: Trust Services Criteria overview page.* AICPA & CIMA
17. EY. *Summary of AICPA revisions to Trust Services Criteria / SOC 2 Description Criteria (2022).* EY
18. MITRE. *ATT&CK Enterprise Cloud Matrix.* MITRE ATT&CK
19. NIST. *SP 800-161r1: Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (Final).* NIST Computer Security Resource Center
20. NIST. *NIST publication page for SP 800-161 (C-SCRM).* NIST
21. NTIA. *Minimum Elements for a Software Bill of Materials (SBOM) (2021).* NTIA
22. Federal Register. *Software Bill of Materials Elements and Considerations (Notice; EO 14028 context).* Federal Register
23. SLSA. *Supply-chain Levels for Software Artifacts (slsa.dev).* SLSA
24. OpenSSF. *SLSA project overview.* OpenSSF
25. CIS. *CIS Critical Security Controls v8 (controls page).* CIS
26. CIS. *CIS Controls v8 white paper (published May 18, 2021).* CIS
27. NIST. *NIST CSF 2.0 overview and purpose statement (publication abstract).* NIST Computer Security Resource Center
28. NIST. *SP 800-53 Rev. 5 control catalog overview (CSRC page).* NIST Computer Security Resource Center
29. CISA. *Secure by Design Pledge (official page).* CISA
30. WIRED. *Reporting on CISA secure-by-design pledge and its objectives (May 2024).* WIRED