

CYBERSMITHSECURE PVT. LTD.

Capability Statement

Art of Cyber Security, Perfected

CERT-In Empanelled

ISO/IEC 27001:2022

ISO 9001:2015

Startup India

CIN U72900MH2019PTC329641 contact@cybersmithsecure.com +91 98231 01337

Nanaji Apartment, Umbergothan, Virar (W) 401301

01

IN THEIR WORDS

Client recommendations

Named, and quoted verbatim.

SECTION 03

Client recommendations

I had the privilege of working closely with Smith Gonsalves and his team during their engagement for Vulnerability Assessments, Penetration Testing, Red Teaming etc. Smith's expertise and meticulous approach to cybersecurity were instrumental in ensuring our systems remained robust and resilient against potential threats.

Arup Mandal

VP — IT, Infosec & Data Privacy, Ather Energy

CyberSmithSECURE has helped us very much in strengthening our defensive as well as offensive capabilities in terms of cyber security. Smith has come through and exceeded all our expectations.

Sneha Joshi

Head of Information Security, Capita

It was a pleasure working with CyberSmithSECURE team who we recommend as the best in managed security services. The Team is very professional and they are dedicated to ensuring 360 degree cyber safety for an organization.

Rajesh Kapase

Director IT, Delhivery

Smith has an eye for detail and a nose to sniff out the more surreptitious vulnerabilities on the network or the system, and his impeccable investigative skills are noteworthy. CyberSmithSECURE services has always added value to SLK Global solutions.

Sanil Nadkarni

CISO & VP, SLK Global

CyberSmithSECURE is one of the most reliable organisations in cyber security consulting arena, we have come across. They are specialized in Red teaming & Penetration testing. They have built up a dedicated team who are innovative and passionate. Their work speaks for themselves.

Sudipta Biswa

CISO & VP, INFOSERV

Trusted by

45 organisations.



02

WHAT WE DO

Services and capabilities

6 service lines, 54 capabilities.

SERVICE PORTFOLIO

GRC

Twenty services, one consistent way of thinking about assurance: understand the requirement, understand the risk, implement the control, and prove that it works.

STANDARDS & COMPLIANCE

ISO 27001 — Gap Assessment	Current-state review against Clauses 4–10 and the Annex A control environment, producing a prioritised gap register and an implementation roadmap rather than a score.
ISO 27001 — Policy & Documentation	The ISMS policies, procedures and records ISO 27001:2022 requires — drafted against your organisational context and mapped to processes that actually run.
ISO 27001 — ISMS Implementation	Building the management system itself — scope, context, governance, risk methodology, risk treatment, Statement of Applicability, policies, procedures, records and operating model.
ISO 27001 — Control Alignment	Translate applicable control guidance into practical ownership, implementation expectations, evidence and monitoring.
ISO 27001 — Certification Support	Readiness for Stage 1 and Stage 2, liaison with the certification body, and structured closure of every finding — with CyberSmithSECURE in the room throughout.
ISO 27001 — Annual Maintenance	Keeping a certified ISMS operating between audits — stewardship, living documentation and year-on-year improvement across the three-year certification cycle.
ISO 27701 — PIMS Implementation	Privacy Information Management System implementation and privacy governance.
ISO 42001 — AI Management System	AI Management System and AI governance implementation.

PRIVACY & DATA PROTECTION

GDPR — GDPR Compliance	CyberSmithSECURE helps organisations assess and establish governance aligned with GDPR requirements.
GDPR — PIA / DPIA	Project-level privacy assessment, applied where processing warrants one.
DPDPA — DPDPA Compliance	Practical governance for personal-data processing under India's Digital Personal Data Protection Act.

SERVICE PORTFOLIO

GRC CONTINUED

SECURITY & COMPLIANCE FRAMEWORKS

NIST CSF — CSF Assessment	Assessment and improvement of cybersecurity governance using the NIST CSF lifecycle.
NIST SP 800-53 — Control Assessment	Control assessment and security governance aligned with NIST SP 800-53.
SOC 2 — Readiness Assessment	SOC 2 readiness and control assessment against applicable Trust Services Criteria.
PCI DSS — Gap Assessment	Payment-card security governance and compliance assessment.
HIPAA — HIPAA Assessment	Security and privacy compliance assessment for organisations subject to HIPAA requirements.

ASSURANCE & RISK SERVICES

Assurance & Risk — Gap Assessment	Assess the organisation's current security, privacy or compliance posture against a defined standard, regulation or framework.
Assurance & Risk — Internal Audit	Independent assessment of the organisation's management system and controls.
Assurance & Risk — Risk Assessment	Identify and evaluate information-security, technology, privacy and business risks.
Assurance & Risk — Third-Party Risk	Assess security and privacy risks introduced by vendors, suppliers and service providers.

BUSINESS RESILIENCE

Business Resilience — Business Impact Analysis	Identify the operational and business consequences of disruption to critical processes, systems and services.
Business Resilience — Continuity Plans	Develop practical continuity plans based on identified business risks and recovery requirements.
Business Resilience — Mock Tests	Test your organisation before a real disruption does. CyberSmithSECURE conducts controlled exercises to evaluate whether business continuity and recovery plans work in practice.

SECURITY LEADERSHIP

vCISO — vCISO Services	Security leadership as a service — strategy, board engagement and programme ownership, from a team rather than a single hire.
-------------------------------	---

SERVICE PORTFOLIO

VAPT

A comprehensive testing approach that identifies vulnerabilities and actively exploits them to assess real security posture.

Web Application	Authenticated, multi-role testing of web applications against OWASP ASVS and the Top 10, focused on business logic and authorisation rather than scanner output.
Android	Static, dynamic and runtime testing of Android applications against OWASP MASVS, including the parts of the attack surface that only exist on a device you do not control.
iOS	Static, dynamic and runtime testing of iOS applications against OWASP MASVS, on jailbroken and stock devices, including the Keychain and App Transport Security behaviour that only appears on real hardware.
API	Testing REST, GraphQL and SOAP interfaces against the OWASP API Security Top 10, with authorisation and object-level access control as the primary focus.
Network	Internal and external network penetration testing against NIST SP 800-115 and PTES, from perimeter enumeration through to lateral movement and domain compromise.
Active Directory	Attack path assessment of on-premises and hybrid Active Directory, from a standard user account to domain compromise, with every path mapped rather than only the first one found.
Cloud	Assessment of AWS, Azure and Google Cloud environments against CIS Benchmarks and the provider's own security reference, focused on identity, privilege escalation paths and exposed data.
Thick Client	Testing of desktop applications — .NET, Java and native Windows — covering the binary, local storage, inter-process communication and the backend the client talks to.
OT / ICS	Passive-first assessment of operational technology and industrial control systems against IEC 62443 and the Purdue model, where availability outranks confidentiality and a scan can stop a production line.
Red Teaming — Full Red Team	Objective-based adversary simulation against people, process and technology, run without the defenders' knowledge, measuring detection and response rather than counting vulnerabilities.
Red Teaming — Assumed Breach	Starts from a foothold already established, so the whole engagement measures what happens after an attacker gets in — which is the question that actually determines the cost of an incident.
Red Teaming — Purple Team	Collaborative technique-by-technique testing with the defenders in the room, measuring detection coverage against MITRE ATT&CK and closing gaps as they are found rather than reporting them later.

SERVICE PORTFOLIO

VAPT CONTINUED

Red Teaming — AI / LLM

Adversarial testing of LLM applications, retrieval pipelines and agent tooling against OWASP LLM Top 10 and MITRE ATLAS, focused on the trust boundaries between a model and the systems it can act on.

Configuration Review

Identifying optimal configurations against CIS benchmarks, because most breaches trace back to misconfiguration rather than an unknown flaw.

Firewall

Rule base and platform review of perimeter and internal firewalls against CIS benchmarks and vendor hardening guides, including the shadowed, redundant and any-any rules that accumulate over years.

Endpoint

Windows, macOS and Linux endpoint hardening reviewed against CIS benchmarks, covering the build, the management policy that maintains it, and whether endpoint protection is configured to actually stop anything.

Microsoft 365

Tenant-wide review of Entra ID, Exchange Online, SharePoint, Teams and Defender against the CIS Microsoft 365 Benchmark, with conditional access and external sharing as the primary focus.

Google Workspace

Review of Google Workspace against the CIS Benchmark, covering admin roles, 2-Step Verification enforcement, Drive sharing, OAuth application access and Gmail security.

Switches & Routers

Hardening review of switches, routers and wireless infrastructure against CIS benchmarks, covering the management plane, VLAN design and the legacy protocols still enabled by default.

IAM & PAM

Review of identity governance and privileged access management — joiner-mover-leaver, entitlement creep, vault coverage and session control — against the accounts that should not still exist.

Backup & Recovery

Review of backup architecture, immutability and restoration capability against the 3-2-1-1-0 rule — because in a ransomware event the backup is the control that decides whether the business pays.

SAP

Review of SAP security configuration — profile parameters, standard users, RFC connections, transport controls and authorisation design — against SAP's own guidance and segregation of duties requirements.

SERVICE PORTFOLIO

Phishing Simulation & Awareness

The human layer is the largest attack surface. We measure it, then improve it.

Mass Phishing

Broad simulated phishing campaigns across the whole organisation, measuring susceptibility by department and over time, with training that follows the click rather than preceding it.

Spear Phishing

Targeted campaigns against named individuals using real open-source intelligence, including executive impersonation and MFA relay, because the attacks that actually cost money are aimed at a handful of people.

Vishing

Telephone-based social engineering against the service desk and staff, testing whether identity verification survives urgency, authority and a convincing caller — including AI voice cloning where authorised.

QR Code

Quishing campaigns delivered by email and by physical placement, testing the attack that moves the target onto an unmanaged personal phone where none of the organisation's controls apply.

Incident Response & Ransomware Recovery

When an incident is live, the priority is containment and getting the business back — analysis comes after.

Ransomware Recovery

Containment, eradication and recovery during a live ransomware event, following the NIST SP 800-61 lifecycle, with getting the business running treated as the first objective and analysis as the second.

Digital Forensics

Evidence-grade investigation of systems, accounts and data movement, with chain of custody maintained throughout so findings hold up in a disciplinary, regulatory or legal process.

Compromise Assessment

A structured hunt across the estate for evidence of a current or past intrusion, answering the question nobody can answer from their dashboards: are we compromised right now.

Vulnerability Fixation

Finding vulnerabilities is the easy part. Most assessments produce a backlog rather than a fix.

Remediation Support

Working the findings closed alongside your teams — validation, prioritisation, and the code or configuration change itself — because an assessment that ends at the report has moved risk to a spreadsheet rather than reducing it.

Verification Retest

Independent retesting of remediated findings, producing evidenced closure rather than an assertion — and catching the fixes that do not work, which is a larger proportion than most organisations expect.

APPROACH AND METHODOLOGY

How an engagement runs

The same seven steps, whichever service line the work sits in.

- 1 Scope & Risk Analysis**
Agree what is in scope, what it is worth, and what would hurt.
- 2 Security Architecture Analysis**
Understand how the environment is built before trying to break it.
- 3 Threat Modeling**
Work out who would attack this, and how they would go about it.
- 4 Test Plan & Preparation**
A written plan, agreed in advance. No surprises during execution.
- 5 Test Execution**
Controlled testing against the agreed scope, evidenced as it goes.
- 6 Document & Report Findings**
Proof, business impact and severity — not a scanner dump.
- 7 Recommend Remediation**
What to fix, in what order, and how to confirm it is fixed.

WHAT YOU RECEIVE

- Executive summary (PDF, one page)
- Technical assessment report (PDF)
- Retest report evidencing closure

03

EVIDENCE

Selected engagements

Anonymised, with the finding, the recommendation and what actually changed.

SECTION 02 · EVIDENCE

GRC

Twenty services, one consistent way of thinking about assurance: understand the requirement, understand the risk, implement the control, and prove that it works.

An EdTech platform with security practices already in place, seeking a structured view of its ISO 27001 position and of what certification readiness would require.

FINDING	Controls were operating, but had never been mapped against ISO 27001:2022 clauses and Annex A in one place — so documentation gaps and evidence gaps blurred into implementation gaps. Documentation was spread across multiple locations, control ownership was interpreted differently across teams, and there were more findings than could be sequenced against the resources available.
RECOMMENDATION	Review the ISMS scope and context alongside the existing policies, procedures and records; assess ISO 27001:2022 clauses and Annex A controls against current organisational practice; hold stakeholder discussions to confirm which controls were operating and where evidence existed; and score maturity by control domain, sequencing remediation by risk, ownership and effort.
OUTCOME	Every gap classified by type — documentation, evidence, ownership or implementation — so remediation effort matched the actual shortfall rather than the finding count. Delivered as a gap assessment report, a clause and control assessment, a risk and gap register, a maturity and readiness view and a remediation roadmap. The organisation's chief executive noted the thoroughness of the assessment of their information security posture.

A SaaS business of around 180 staff, certifying to unblock enterprise sales.

FINDING	The initial scope proposed covered the whole company. Assessment showed the enterprise customers driving the requirement only cared about the production platform and the people who touch it — roughly a third of the organisation.
RECOMMENDATION	Narrow the scope to the platform and its supporting functions, with clearly documented boundaries and interfaces, and extend later if customers ask.
OUTCOME	Certification achieved in five months rather than the projected eleven. Representative pattern; details illustrative and not attributable to a named client.

SECTION 02 · EVIDENCE

GRC CONTINUED**A manufacturer that had failed a certification audit under a previous provider.**

FINDING	A complete, well-written document set with almost no operating evidence. The risk register had not been reviewed since creation, no internal audit had been run, and management review existed as a single undated slide.
RECOMMENDATION	Stop producing documents. Run the processes for one full quarter — risk review, access review, incident handling, supplier review — and let the evidence accumulate naturally before rebooking the audit.
OUTCOME	Certified at the second attempt. The organisation's own conclusion was that the first programme had optimised for the wrong deliverable. Representative pattern; details illustrative.

SECTION 02 · EVIDENCE

VAPT

A comprehensive testing approach that identifies vulnerabilities and actively exploits them to assess real security posture.

A B2B SaaS platform serving around 400 corporate tenants.

FINDING	Tenant identifier was accepted from a request header and trusted. Changing it returned another tenant's user list, invoices and uploaded documents, from any authenticated account on any tenant.
RECOMMENDATION	Derive tenant context from the session server-side and never from client-supplied input. Add a tenant-isolation test to the regression suite so the class cannot return.
OUTCOME	Fixed within a week and verified by retest. The regression test caught a similar issue on a new endpoint four months later.

An insurance portal handling policy purchase and claims.

FINDING	The premium was calculated client-side and submitted with the order. Intercepting and reducing it produced a valid policy at the attacker's price, because the server re-validated the policy but not the amount.
RECOMMENDATION	Recalculate every monetary value server-side at the point of transaction and treat client-submitted amounts as display data only.
OUTCOME	Recalculation moved server-side. A reconciliation check against historical orders found no prior abuse, which is what made the finding closable rather than an incident.

A public sector grievance portal, roughly 90,000 registered citizens.

FINDING	Password reset tokens were derived from a timestamp and were six digits. With no rate limit on the reset endpoint, any account could be taken over in under ten minutes of automated guessing.
RECOMMENDATION	Cryptographically random tokens of at least 128 bits, single use, 15-minute expiry, with rate limiting and alerting on the reset endpoint.
OUTCOME	Implemented before public disclosure was necessary. Rate limiting was extended to authentication endpoints generally, which also reduced credential-stuffing traffic.

SECTION 02 · EVIDENCE

Configuration Review

Identifying optimal configurations against CIS benchmarks, because most breaches trace back to misconfiguration rather than an unknown flaw.

A retail group with 140 stores behind a central perimeter pair.

FINDING	The rule base had grown to 1,840 rules over eleven years. Analysis found 312 shadowed rules that could never match, 96 with no logging, and an any-any rule between the store network and the card data environment added during a 2019 migration and never removed.
RECOMMENDATION	Remove the any-any rule immediately with a narrow replacement, then run a staged clean-up of shadowed and unlogged rules against hit count evidence.
OUTCOME	The any-any rule was replaced within 24 hours. Clean-up removed 430 rules over three months with no service impact, and the base is now reviewed quarterly.

A manufacturer running Fortinet at the perimeter and Cisco ASA internally.

FINDING	Each device passed its own vendor review. Normalising both rule bases into one model showed that a permitted flow through the perimeter, combined with an internal rule, allowed a supplier VPN to reach the plant historian — a path neither review saw in isolation.
RECOMMENDATION	Assess the estate as one policy rather than device by device, and add an explicit deny between supplier VPN and any OT-adjacent zone.
OUTCOME	Deny rule added at the next change window. Reviews are now scoped across the estate rather than per device.

A financial services firm preparing for a PCI DSS assessment.

FINDING	Management interfaces on both perimeter firewalls accepted connections from the general user VLAN, and administrative accounts were local with no MFA. The six-monthly rule review required by PCI had been recorded as complete but produced no evidence.
RECOMMENDATION	Restrict management to a dedicated administrative network, federate administrative authentication with MFA, and produce a documented review with rule dispositions as the evidence artefact.
OUTCOME	All three completed before the assessment. The documented review became the template for subsequent cycles, which is what made the control sustainable rather than a one-off.

SECTION 02 · EVIDENCE

Phishing Simulation & Awareness

The human layer is the largest attack surface. We measure it, then improve it.

A professional services firm of around 800 staff running its first programme.

FINDING	The baseline returned a 31% click rate and a 4% report rate. The report button existed in Outlook but sent reports to a shared mailbox nobody monitored; three genuine phishing emails reported by staff in the preceding quarter had gone unread.
RECOMMENDATION	Route reports to the security team with a triage SLA, acknowledge every report to the reporter, and make report rate the headline metric in management reporting.
OUTCOME	Report rate reached 38% within three quarters and click rate fell to 12%. The acknowledgement loop was, per staff feedback, the single change that made people bother.

A manufacturer with plant and office staff.

FINDING	The organisational click rate of 14% concealed a 6% office rate and a 41% rate among plant supervisors, who used shared terminals, had minimal email experience and had never received training because the programme assumed desk-based staff.
RECOMMENDATION	Build role-specific training for shared-terminal users, and report by population rather than as a single organisational figure.
OUTCOME	Supervisor click rate fell to 17% over two quarters. Reporting by population is what made the gap visible after it had been invisible in the aggregate for two years.

A financial services firm that had run simulations for three years with improving numbers.

FINDING	Click rate had fallen from 22% to 4%, which the board saw as success. Review found every campaign had used the same platform's default templates, and staff recognised the sender pattern. A campaign using a bespoke template matched to the client's own systems returned 27%.
RECOMMENDATION	Vary templates and senders, declare difficulty, and treat the previous three years of trend data as measuring template familiarity rather than resilience.
OUTCOME	The programme was redesigned with graded difficulty. Restating the trend honestly to the board was uncomfortable and led to funding for role-based training that the false trend had made look unnecessary.

SECTION 02 · EVIDENCE

Incident Response & Ransomware Recovery

When an incident is live, the priority is containment and getting the business back — analysis comes after.

A manufacturing group, roughly 1,100 endpoints, encrypted across two sites overnight.

FINDING	Initial access was a VPN appliance unpatched against a known exploited vulnerability, with a dwell time of 23 days. Backups were encrypted because the backup server was domain-joined and the service account held domain administrator. 340 GB had been exfiltrated to cloud storage over the preceding week.
RECOMMENDATION	Recover from the one offline tape set, rebuild domain controllers from clean media, separate backup identity from the production domain, and notify under the applicable obligations given the confirmed exfiltration.
OUTCOME	Production was running on critical systems within nine days and fully recovered in five weeks, with four days of data loss. The exfiltration evidence determined the notification position, which the client would otherwise have got wrong.

A hospital group, ransomware affecting administrative systems with clinical systems unaffected.

FINDING	Containment stopped spread before clinical networks were reached — segmentation implemented two years earlier held. Initial access was a contractor account with no MFA. Backups were intact and immutable.
RECOMMENDATION	Recover from backup, enforce MFA on all third-party access, and review every contractor account for necessity and privilege.
OUTCOME	Full recovery in six days with no clinical impact. The segmentation that limited the blast radius had been a finding from a prior assessment, which the board noted when approving the next security budget.

A logistics company that had contained an incident itself before calling.

FINDING	Containment had been effective but incomplete: a scheduled task on two non-obvious hosts survived and would have re-established access. Systems had also been restored into the original network segment without verification, and the initial access route remained open.
RECOMMENDATION	Complete eradication across the full estate rather than the affected hosts, close the entry route before reconnecting anything, and re-verify every restored system.
OUTCOME	The surviving persistence was removed before it activated. The client's own view was that self-containment had been the right first move and that stopping there would have cost them the recovery.

SECTION 02 · EVIDENCE

Vulnerability Fixation

Finding vulnerabilities is the easy part. Most assessments produce a backlog rather than a fix.

A fintech with 1,400 open findings accumulated across two years of assessments and scanning.

FINDING	Validation discarded 380 as false positives or no longer applicable. Root cause grouping reduced the remaining 1,020 to 47 underlying causes; the largest, a missing authorisation helper, accounted for 211 findings across one codebase.
RECOMMENDATION	Fix by root cause. Implement the authorisation helper once, apply it across all 211 call sites, and add a lint rule preventing new endpoints without it.
OUTCOME	The backlog fell from 1,400 to 190 in one quarter. The lint rule is what stopped it regrowing — the following year's assessment found four instances rather than the expected hundreds.

A manufacturer with a vulnerability management programme reporting 94% patch compliance.

FINDING	The 6% outstanding contained every internet-facing system and four appliances on the CISA known-exploited list, because those systems were hardest to patch and had been repeatedly deferred. Compliance was measured by host count, so deferring the difficult ones improved the figure.
RECOMMENDATION	Weight compliance reporting by exposure and criticality rather than host count, and treat known-exploited vulnerabilities as a separate track with its own SLA.
OUTCOME	All known-exploited items closed within six weeks once they were visible. The measurement change was the actual fix; the previous metric had been rewarding the wrong behaviour.

A healthcare provider where the same findings recurred in three consecutive annual assessments.

FINDING	Findings were assigned to an IT team with no capacity and no application knowledge. Nothing was ever verified, so items were closed on assertion and reappeared the following year. The register had lost all credibility internally.
RECOMMENDATION	Rebuild the register with validated findings only, assign by capability rather than by department, and require verification evidence before closure.
OUTCOME	Closure rate went from 31% to 88% over two quarters. The verification requirement caught nine fixes that had not worked, all of which had been recorded as complete the previous year.

GET IN TOUCH

Contact

EMAIL

contact@cybersmithsecure.com

TELEPHONE

+91 98231 01337

Offices

INDIA · MUMBAI

511, Ascot Centre
Mumbai 400099

INDIA · REGISTERED

Nanaji Apartment, Umbergothan
Virar (W) 401301

USA · NEW JERSEY

381 Blair Road
Avenel, NJ 07001

CANADA · ONTARIO

Suite 750, 2 Robert Speck Pkwy
Mississauga, ON L4Z 1H8

UK · GLASGOW

50 Mossbank Drive
Glasgow G33 1LS

KSA · AL KHOBAR

Al Khobar 31952
P.O. Box 4607

UAE · DUBAI

308 Indigo Tower, Cluster D
JLT, Dubai, P.O. Box 112965