CyberSentien

How every capability helps you

A practical guide to CyberSentien, one capability at a time: the problem it solves, what it does, and what changes for you. Readiness assessments, continuous monitoring, AI governance and security leadership in one engine. Built in Australia. Runs on your own server or cloud, so your evidence stays with you.

76
frameworks across Australia, the US, UK, Canada, New Zealand and the EU, with 14 more coming soon

342
CIS Benchmarks for operating systems, cloud, databases and devices, coming soon

>98%
of the AI's credits currently correct on blind tests

63
connectors, all read-only, including 78 Microsoft 365 collectors

Every
output sealed in a tamper-evident, hash-chained ledger

Yours
runs on your own server or cloud, with local AI

LIVE DEMO
demo.cybersentien.com

SAMPLE REPORTS
cybersentien.com/sample-reports

GUARDIAN CONSOLE
guardian.cybersentien.com/console

CONTENTS

Inside this guide

Each chapter follows the same pattern: the challenge you face, what CyberSentien does about it, and what that means for your team, your board and your auditor.

1 Readiness assessments 5

2 Accuracy you can defend 6

3 Reports and auditor handoff 7

4 ISM and IRAP 8

5 Board packs 9

6 Strategist 10

7 Ask CyberSentien 11

8 Continuous monitoring and connectors 12

9 Remediation and live view 13

10 GRC registers 14

11 Third-party risk management 15

12 Retail 16

13 Fraud and AML 17

14 Incident response 18

15 Attack and defence 19

16 CyberSentien Guardian 20

17 AI governance 21

18 Video calls into evidence 22

19 Questionnaires and trust centre 23

20 Consultants, practices and MSSPs 24

21 Expert directory 25

22 Tamper-evident seal and audit trail 26

23 Architecture and deployment 27

Who it serves 28

Also included 29

Framework catalogue 30

CIS Benchmark library 31

On the roadmap 32

Getting started 33

WHY CYBERSENTIEN

Compliance should not cost your team its evenings

Security and compliance teams carry a heavy load: framework after framework, evidence spread across systems, questionnaires from every customer, board papers every quarter and a regulator clock that never stops. Most of that time goes on gathering, checking and rewriting, not on making the organisation safer.

Evidence everywhere

Policies, registers and system settings sit in different places, and every assessment starts by chasing them again.

Answers you cannot prove

Tools that match keywords give false comfort that falls apart in front of the auditor.

Reports out of date on arrival

A snapshot assessment says nothing about the setting that changed last week.

Too many audiences

The board, the regulator, customers and auditors each want the same facts in a different shape.

What changes with CyberSentien

CyberSentien reads your evidence against the intent of every control, the way an experienced assessor does, and shows the exact passage or live setting behind every result. Evidence is collected once and answers every framework you choose. Connected systems keep it current. Reports, board packs and questionnaires come from the same evidence, sealed so no one can quietly change them. Anything uncertain goes to a person with the reason, so you are never asked to trust a guess.

FOR YOUR TEAM
Time back from evidence chasing and report writing

FOR YOUR BOARD
Clear, evidence-backed decisions

FOR YOUR AUDITOR
A pack they can work from on day one

CyberSentien performs readiness assessments. It prepares you for certification or attestation and hands your auditor a ready pack; the certification itself comes from your auditor.

WHAT CYBERSENTIEN IS

An expert assessor's reading, at machine speed

CyberSentien reads your evidence against the intent of every control, the way an experienced assessor does. It shows the exact passage or live setting behind every result, and anything it is not sure about goes to a person with the evidence and the reason.

1. Bring your evidence

Upload the policies, registers and system reports you already have, connect the systems you already run, or capture it on a recorded video call.

2. Every control read

Each requirement is shown as ready, partly ready or missing, with the quoted passage it rests on and what to add next.

3. Reports you can defend

Board, technical and auditor-handoff reports, a remediation project plan, and a seal anyone can verify offline.

How correctness is proven

Settled answers, unseen tests

For each framework, test sets of evidence matched to requirements are built with settled answers. The AI is tested on sets it has never seen, and every credit it gives is counted right or wrong.

Sure-only credits

A control is credited only when the evidence clearly proves it. Everything less certain becomes "candidate evidence, assessor review", never a guess. A wrong pass is treated as seriously as a wrong fail.

Locked versions

The AI's exact version is pinned by digest. A new version gives credits only after passing a fresh test above 95% correct, so accuracy cannot quietly slip.

Numbers from evidence only

Every figure on every screen comes from your evidence or says "unknown". Nothing is invented to fill a gap.

Deployment and data sovereignty

Your server or your cloud

- Install pack and step-by-step guide; launchers for Windows, macOS and Linux
- Your evidence never has to leave your environment
- Australian-hosted option for organisations that prefer it

CyberSentien's proprietary AI, tuned in-house

- Runs locally: CPU mode on an ordinary server, or GPU mode on your own graphics card (24 GB minimum, 48 GB recommended)
- Every AI read records where it ran; customer evidence never goes to rented compute

> CyberSentien performs readiness assessments. It prepares you for your certification or attestation and hands your auditor a pack they can work from; it does not issue certifications.

Know exactly where you stand, control by control

THE CHALLENGE

A readiness assessment usually means weeks of chasing documents, a spreadsheet nobody trusts, and a consultant's view that is out of date by the time it lands. When the auditor arrives, the team is still guessing which controls will hold up.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Every control shown as ready, partly ready or missing, with the reason and what to add	→ **You stop guessing. The team sees the true position and the next step for each requirement.**
Each finding links to the exact document and passage it rests on	→ **Anyone can check a result in seconds, so internal debates turn into quick decisions.**
The same evidence answers every framework you choose	→ **Evidence collected once serves ISO 27001, SOC 2, CPS 234 and more, so nothing is gathered twice.**
Controls with no evidence are counted apart from real findings	→ **A thin submission reads as a gap to fill, not as a poor security posture.**
ISO 27001 Statement of Applicability, scope and boundary set per engagement	→ **The documents an assessor expects are ready from the start.**
Evidence library keeps each document's name, owner, date and version	→ **You always know which version was used and who owns it.**

IN PRACTICE

A compliance lead uploads the policies and registers the team already has and connects Microsoft 365. The engine reads every control and lists what is ready, what is partly there and what is missing, each with the passage behind it. The lead sends the gap list to owners the same week, instead of building a spreadsheet first.

OUTCOME
A clear, defensible position, fast

OUTCOME
Less consultant time spent on evidence gathering

OUTCOME
Walk into the audit knowing the answer

WHO IT IS FOR

Compliance leads, CISOs, risk teams and consultants running assessments

SEE IT FOR YOURSELF

Sample reports: cybersentien.com/sample-reports.html

Results you can put your name to

THE CHALLENGE

Automated compliance tools often say a control passes because a keyword appears in a policy. That false comfort is worse than no answer, because it fails in front of the auditor or the regulator.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
CyberSentien's proprietary AI, tuned in-house, reads evidence against the intent of each control	→ **Results reflect what the evidence actually proves, the way an experienced assessor reads it.**
Currently more than 98% of the AI's credits are correct on blind tests	→ **You can rely on what is shown as met, and spend review time where it matters.**
A control is credited only when the evidence clearly proves it	→ **No false greens. Uncertain cases become "candidate evidence, assessor review" with the reason.**
A wrong pass is treated as seriously as a wrong fail	→ **You are never told you are in worse shape than you are, either.**
The AI's exact version is pinned; a new version gives credits only after a fresh test	→ **Accuracy cannot quietly slip between assessments.**
Every number on every screen comes from evidence, or says "unknown"	→ **Nothing is invented to fill a gap, so every figure survives scrutiny.**

IN PRACTICE

An assessor opens a result marked as met and clicks through to the quoted passage that proves it. A second control the AI was unsure about sits in the review queue with its candidate documents and the reason. The assessor spends time only on that one, and signs off the rest with confidence.

OUTCOME
Confidence in every result shown

OUTCOME
Reviewers focus on the uncertain cases only

OUTCOME
Results that stand up to an auditor

WHO IT IS FOR

Anyone who signs off on compliance results

SEE IT FOR YOURSELF

Live demo: demo.cybersentien.com

Reports your auditor can work from on day one

THE CHALLENGE

Writing a readiness report by hand takes days, and the result is often a long document that tells the board little and gives the auditor even less to work from.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Framework readiness reports for every pack: CPS 234, SOC 1 and 2, ISO 27001, ISM/IRAP, PCI DSS, NIST CSF, FedRAMP, Essential Eight and more	→ **A finished, professional report from the evidence you already hold.**
Auditor handoff pack included with every report bought	→ **Your auditor starts from an organised pack, which shortens fieldwork.**
"Ready for your auditor" one-page action plan at the front	→ **Leaders see what must happen next on a single page.**
Remediation project plan with phases, owner roles, dates and milestones	→ **The report turns straight into a plan the team can run.**
Indicative financial exposure from cited statutes and your turnover	→ **The board sees why a gap matters in dollars, from cited law, never a prediction.**
MITRE ATT&CK techniques left open by gaps, and Microsoft Secure Score compared with what evidence proves	→ **Technical teams see the real-world risk behind each gap.**
English and Arabic reports, with right-to-left layout	→ **Serve clients and regulators in the language they work in.**

IN PRACTICE

After the assessment, the team generates the ISO 27001 readiness report. The one-page action plan goes to the executive, the remediation plan goes to the project lead, and the auditor handoff pack goes to the external auditor, all from the same sealed evidence.

OUTCOME
Days of report writing handed back to the team

OUTCOME
A smoother, shorter audit

OUTCOME
One evidence base, many audiences

WHO IT IS FOR

Compliance teams, consultants and practices that deliver reports

SEE IT FOR YOURSELF

Read the 32 to 734-page samples at cybersentien.com/sample-reports.html

An IRAP-ready assessment, end to end

THE CHALLENGE

The ISM is large, detailed and changes every quarter. Preparing for IRAP by hand ties up a team for months, and look-alike evidence is easily credited to the wrong control.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Every ISM control on ASD's September 2026 release, with the June 2026 edition kept on record	→ **You assess against the current manual and can still show the previous one.**
Applicability by classification and system, with scope and boundary per engagement	→ **Only the controls that apply to your system are in front of you.**
ISM-specific subject checks stop look-alike evidence being credited	→ **Each credit rests on evidence about the right subject.**
Security Assessment Report, executive brief, evidence pack and boundary diagram	→ **The deliverables an IRAP assessor expects, already structured.**
Residual-risk register, assessor opinion and authorisation recommendation	→ **The decision maker gets what they need to authorise the system.**
Documents checked against what Microsoft 365, Entra, Intune and Defender actually show	→ **A policy that says MFA is enforced, on a tenant where it is not, is caught before the assessor finds it.**

IN PRACTICE

An agency preparing for IRAP sets its classification and system boundary. The engine shows only the ISM controls that apply, checks the security policy against what Entra and Intune actually enforce, and drafts the Security Assessment Report structure. The IRAP assessor starts from a complete pack rather than an empty template.

OUTCOME
Months of preparation shortened

OUTCOME
Fewer surprises in the IRAP assessment

OUTCOME
The assessor keeps control, with a strong starting point

WHO IT IS FOR

Government agencies, defence suppliers, cloud providers and IRAP assessors

SEE IT FOR YOURSELF

734-page sample ISM IRAP report at cybersentien.com/sample-reports.html

What the board needs, from the evidence itself

THE CHALLENGE

Board papers on cyber are often slides built from opinion, assembled the night before. Directors can't tell what changed, what it means, or what they must decide.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Board and regulator assurance pack, focused for the board risk or audit committee, CISO, CRO or APRA	→ **Each reader gets the view that suits their role, from one source.**
Posture across every framework you answer to, with top exceptions and a short reason for each	→ **Directors see the few things that matter, in plain words.**
Continuous drift since the last pack	→ **The board sees what has changed, not just a snapshot.**
Executive pack in red, amber and green, in colours and shapes that also print in black and white	→ **Easy to read in the meeting and in print.**
Quarterly strategist briefing and a 12-month plan with cost bands	→ **The board gets a plan and a budget conversation, not just a status.**
Every figure computed from collected evidence and sealed	→ **Numbers a director reads are numbers an assessor can trace.**

IN PRACTICE

The night before a board risk committee, the CISO generates the board assurance pack instead of building slides. Directors see posture across every framework, the top exceptions with a reason each, and what has drifted since last quarter, with every figure traceable.

OUTCOME
Board papers without the late nights

OUTCOME
Clear decisions for directors

OUTCOME
Evidence-backed answers for the regulator

WHO IT IS FOR

CISOs, CROs, company secretaries and board committees

SEE IT FOR YOURSELF

Ask for a sample board pack

CHAPTER 6 · STRATEGIST

A security adviser that never stops watching

THE CHALLENGE

Most organisations can't afford a full-time senior security leader, and those that have one find them buried in reporting instead of steering.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Security plan, board view and follow-ups, with exposure by attack type in red, amber and green	→ **Leadership-level advice on what matters most, every day.**
Every colour comes from a printed rule, and grey means the answer is unknown	→ **You can see why something is red, and trust that green is earned.**
Tells the board what it must decide, and what is being watched	→ **Meetings move from status updates to decisions.**
Joins attack drills with live Microsoft 365, Entra, Intune and Defender readings	→ **Advice reflects your environment as it is today.**
Expert directory for vCISO, IRAP, QSA and lead-auditor help when a gap needs a person	→ **When you need a human expert, the right one is a click away.**

IN PRACTICE

Monday morning, the Strategist turns phishing exposure amber because two admin accounts lost MFA over the weekend. It names the fix, the owner and what the board needs to know. The security lead acts on one clear recommendation instead of reading a dashboard.

OUTCOME
Senior security guidance without a senior headcount

OUTCOME
A plan the board understands

OUTCOME
Time back for your security lead

WHO IT IS FOR
Mid-sized organisations, CISOs and vCISOs

SEE IT FOR YOURSELF
Strategist in the live demo

Ask a question, get an answer you can cite

THE CHALLENGE

Finding the one sentence that proves a control means searching hundreds of pages. Teams answer the same questions again and again for auditors, customers and the board.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Plain-language questions answered with the quoted passage or live setting behind each answer	→ **You get the answer and the proof together.**
Knows every framework in the catalogue and your own Microsoft 365 configuration	→ **One place to ask about rules and about your environment.**
Unsure answers say so and go to a person	→ **You never act on a guess.**
Follow-up questions keep the context of the engagement	→ **Work through a topic naturally, without starting again.**
Answers feed working papers, questionnaires and the Strategist	→ **An answer found once is reused everywhere it is needed.**

IN PRACTICE

An auditor asks whether backups are tested. The consultant types the question into Ask and gets the answer with the quoted line from the backup procedure and the date of the last restore test. The answer goes straight into the working papers.

OUTCOME
Hours of document searching handed back

OUTCOME
Consistent answers across teams

OUTCOME
Every answer traceable

WHO IT IS FOR
Assessors, consultants, security and compliance teams

SEE IT FOR YOURSELF
Try Ask in the live demo

Assurance that stays current between audits

THE CHALLENGE

An assessment is a snapshot. A week later a setting changes, an admin loses MFA, and the report no longer describes the organisation.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
63 read-only connectors, including 78 Microsoft 365 collectors	→ **Evidence comes straight from the systems you run, with no manual exports.**
Microsoft 365, Entra, Intune, Defender, Sentinel; AWS, Azure, Google Cloud; Okta, CrowdStrike, Tenable, Qualys, GitHub, ServiceNow and more	→ **Your existing tools become live evidence sources.**
Entra conditional access analysis, including report-only MFA policies that look green but are not	→ **Hidden gaps that fool dashboards are found.**
Sources re-polled on a schedule, with drift tracked	→ **You know the day something changes, not at the next audit.**
Every connector is read-only	→ **Your environment stays exactly as your team set it.**
A connector check that passes is a credit you can rely on	→ **Live settings prove controls without a document.**

IN PRACTICE

A cloud engineer makes a storage bucket public late on a Friday. At the next scheduled poll the drift appears on the dashboard and the affected controls move. The team corrects it on Monday, long before the next audit would have found it.

OUTCOME
Always-current assurance

OUTCOME
Drift caught early

OUTCOME
Less manual evidence collection

WHO IT IS FOR

IT and security teams, MSSPs and organisations with continuous compliance duties

SEE IT FOR YOURSELF

Connector list in the full catalogue

From gap to fix, and a live picture all the way

THE CHALLENGE

Knowing the gaps is only half the job. Teams need to know what to fix first, who owns it, and when it is truly done.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
For each control: what is missing and what to add, from the control's own evidence requirements	→ **Every gap comes with a clear next step.**
Remediation plan: unmet controls in days 0 to 30, partly met in days 30 to 90, with owners and milestones	→ **A ready-made project plan the team can start on.**
The fixes that break the most attack paths, ranked	→ **Effort goes where it reduces the most risk.**
Clarification loop and secure upload links for missing evidence	→ **Questions reach the client precisely, and answers come straight back as evidence.**
What-if scenarios before you start	→ **See the effect of a set of fixes before committing the budget.**
Overview dashboard with tiles per organisation, updated as evidence arrives	→ **Everyone sees current progress, not last quarter's.**

IN PRACTICE

After the assessment, the project lead opens the remediation plan: the most important unmet controls are scheduled first, each with an owner role and target date. As fixes land and evidence arrives, the dashboard updates, and the engine re-check proves each fix is done.

OUTCOME
A plan on day one

OUTCOME
Fixes proven, not assumed

OUTCOME
Live progress for leaders

WHO IT IS FOR
Security managers, project leads and consultants

SEE IT FOR YOURSELF
Live dashboard in the demo

The registers a regulated organisation keeps, built in

THE CHALLENGE

Risk registers, supplier lists, BIAs and retention schedules often live in separate spreadsheets that drift apart and never link to the controls they support.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Risk and residual-risk registers with the assessor's opinion	→ **Risk lives next to the evidence that supports it.**
CPS 230 critical operations, impact tolerances, material service providers, BIA and DR exercises	→ **Operational resilience obligations met in one place.**
Data asset register, retention, legal hold and investigation register	→ **Records are defensible, and held evidence can't be deleted or aged out.**
Privileged access assurance, firewall rule analysis and Defender CVEs mapped to assets	→ **Technical assurance from live data.**
SBOM and VEX register, DevSecOps scanner results and secure development gates	→ **Software supply chain risk becomes evidence.**
Obligations linked to the controls that meet them, with crosswalks between frameworks	→ **See which law each control satisfies, once.**

IN PRACTICE

A bank's resilience team keeps its CPS 230 critical operations, tolerances and material service providers in CyberSentien. When a supplier changes, the register, the linked controls and the board pack all reflect it, instead of three spreadsheets drifting apart.

OUTCOME
One connected GRC system

OUTCOME
Fewer spreadsheets

OUTCOME
Registers that stay in step with evidence

WHO IT IS FOR

Risk, compliance and resilience teams in regulated sectors

SEE IT FOR YOURSELF

Registers in the live demo

Know every supplier, from both sides

THE CHALLENGE

Supplier questionnaires go out by email, answers come back late, and nobody notices when a key supplier is breached or deregistered.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Supplier register and tracker with owners, criticality and renewal dates	→ **Every supplier and its risk in one view.**
22-question standard set, CPS 234 and CPS 230 sets, and the full set, with automatic reminders and escalations	→ **Questionnaires chase themselves.**
Public warning signs: breach history, sanctions (OFAC, UN, DFAT), ASIC status, domain health and news	→ **You hear about supplier trouble early.**
Five-page supplier board report and CPS 230 material service provider export	→ **Board and APRA reporting comes ready.**
Supplier Pack: one profile and trust page shared with every customer	→ **Suppliers answer once and share many times, which wins business.**
Supplier evidence kept by link and fingerprint, sealed in the ledger	→ **Files stay with the supplier, and nothing can be swapped later.**

IN PRACTICE

A new payments supplier is onboarded. The CPS 230 questionnaire goes out automatically, reminders chase it, and public signals show a recent domain change worth asking about. The board report lights the supplier amber until the answers come back.

OUTCOME
Faster supplier onboarding

OUTCOME
Early warning on supplier risk

OUTCOME
Smaller suppliers win larger customers

WHO IT IS FOR

Procurement, vendor risk teams, and suppliers to regulated organisations

SEE IT FOR YOURSELF

Supplier Pack and tracker in the demo

Built for the way attackers now target retail

THE CHALLENGE

Retailers are being hit through the help desk, through customer and loyalty logins, and by ransomware with new reporting duties, while in-store facial recognition draws privacy scrutiny.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
A Retail Command Centre console of its own, built for retailers rather than banks	→ **Your team works in a view made for retail, with its own sample retailer to explore.**
Help-desk reset checklist: identity checks an attacker cannot look up, stronger checks for admins, every reset recorded	→ **Closes the route attackers have used to talk their way past staff help desks.**
Customer and loyalty login checklist: bot and credential-stuffing defences, breached passwords refused, takeover and points fraud watched	→ **Protects customer accounts and the value stored in loyalty points.**
Ransomware payment reporting checklist under the Cyber Security Act 2024: who decides, the 72-hour report in the incident plan, rehearsed	→ **You are ready for the reporting duty before you ever need it.**
In-store facial recognition checklist: a register of every deployment, notice, necessity, retention and a person reviewing before acting	→ **Use biometrics with the privacy safeguards the regulator expects.**
Guardian's retail pack holds AI-agent moves of points, gift cards and store credit, bulk exports and refunds for a person, and refuses refund bursts; every decision sealed	→ **AI agents in your stores and service desk can't be turned into a fraud channel.**

IN PRACTICE

A retailer's security lead opens the Retail Command Centre and works through the help-desk checklist. Two items are gaps: executives can reset with the same checks as everyone else, and resets raise no alert. The fixes go into the remediation plan, and Guardian's retail pack stops the service-desk AI agent moving gift-card balances without a person's approval.

OUTCOME
Defences aimed at today's retail attacks

OUTCOME
Ready for ransomware reporting

OUTCOME
Loyalty and gift-card value protected

WHO IT IS FOR

Retailers, shopping centres, loyalty programs and their MSSPs

SEE IT FOR YOURSELF

Retail Command Centre: demo.cybersentien.com/ui/retail

Fraud and AML obligations, evidenced end to end

THE CHALLENGE

AML/CTF programs are judged on evidence. Fraud tools produce alerts, but the program around them often lives in documents nobody can trace to a control.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
A Fraud and AML pack of 18 controls on the AUSTRAC AML/CTF obligations, from risk assessment and due diligence to SMR and TTR reporting, sanctions, travel rule and independent evaluation, with an evidence-led status for each	→ **The whole program is assessed against what AUSTRAC expects, at a glance.**
Connect points for your core-banking feed, payments switch, transaction monitoring, sanctions and PEP screening, and fraud or decisioning engine	→ **Your existing fraud and AML tools feed the assurance picture directly.**
Live detection tiles light up only from a connected feed; until then they say "not connected"	→ **Every alert or count you see comes from your own systems, so it stands up.**
Fraud events kept in the incident and event registers; fraud-detection controls collected from your SIEM	→ **Fraud incidents are tracked to closure with the rest of your risk.**
Fraud-detection and credit models governed in the AI register, with impact, bias and drift checks	→ **The models behind fraud decisions are themselves under control.**
Sanctions screening (OFAC, UN, DFAT) on suppliers, and Guardian holding refund and stored-value moves by AI agents	→ **Fraud risk is covered across customers, suppliers and AI.**

IN PRACTICE

A lender preparing for its independent AML/CTF evaluation uploads its program, risk assessment, due diligence procedures and reporting records. The posture view shows threshold reporting and sanctions screening as evidenced, and flags that the risk assessment is out of date. The evaluator receives a sealed pack with each control's evidence attached.

OUTCOME
An evaluation-ready AML/CTF program

OUTCOME
Fraud tools tied to obligations

OUTCOME
Every figure from your own systems

WHO IT IS FOR

Banks, lenders, brokers, payments and remittance businesses

SEE IT FOR YOURSELF

Fraud and AML view in the bank console: demo.cybersentien.com/ui/bank

Every incident run to closure, every deadline met

THE CHALLENGE

When an incident hits, teams juggle alerts, emails and regulator deadlines at once. A missed 72-hour notice turns a security incident into a regulatory one.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Defender, Sentinel and identity-risk alerts become draft incidents for a person to confirm	→ **Nothing slips through, and nothing is invented.**
Full lifecycle: triage, contain, eradicate, recover, post-incident review, each time-stamped	→ **A complete, defensible record of every case.**
Regulator clocks: APRA CPS 234 (72 hours), SOCI (12 and 72 hours), OAIC (30-day assessment), EU AI Act Article 73	→ **The deadlines that apply to you are always in view.**
Communications trail, affected assets and controls on every case	→ **Post-incident questions are answered from the record.**
Lessons learned carried into the remediation plan	→ **Each incident leaves you stronger.**
Investigation register and legal hold	→ **Evidence is preserved for lawyers and regulators.**

IN PRACTICE

A Defender alert becomes a draft incident. The analyst confirms it, the CPS 234 72-hour clock appears with the provision's own wording, and every step from containment to post-incident review is time-stamped. The lessons learned flow into the remediation plan.

OUTCOME
Regulator deadlines met

OUTCOME
Calmer, faster response

OUTCOME
Incidents that improve security

WHO IT IS FOR
Security operations, risk and legal teams

SEE IT FOR YOURSELF
Incident register in the demo

See how an attacker would get in, and close the path

THE CHALLENGE

Long lists of vulnerabilities don't tell you which fix matters most. Meanwhile attackers chain small weaknesses into one open path.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Each attack type traced stage by stage, from live Microsoft 365, Entra, Intune and Defender readings	→ **You see the real paths into your organisation.**
Every path shown as open, likely open, broken or showing attack signs	→ **Priorities are obvious at a glance.**
Choke points ranked by how many paths one fix breaks	→ **The smallest effort for the biggest risk reduction.**
A fix counts as proven only on re-check, and the proof is sealed	→ **You can show the board that a path is closed.**
MITRE ATT&CK and ATLAS alignment in every report	→ **Speaks the language your security team already uses.**
CyberSentien's own security lab: a web firewall, intrusion detection and a SIEM under repeated published attacks, with Guardian later built on top of it and tested the same way; every lab result is fed to the engine as evidence	→ **You see proof that defences work, not just that you own them.**

IN PRACTICE

The engine finds an attack path: an admin without MFA, legacy sign-ins still allowed, and an open high-severity incident. It shows that one conditional access fix breaks three paths at once. After the fix, the re-check marks the path broken and seals the proof for the board.

OUTCOME
Fewer open attack paths

OUTCOME
Fix budgets spent where they count

OUTCOME
Proof that fixes worked

WHO IT IS FOR

CISOs, security engineers and MSSPs

SEE IT FOR YOURSELF

Attack paths in the Strategist

Use AI agents safely, with a guard on every action

THE CHALLENGE

AI agents can now send email, query databases and call tools. One poisoned document or prompt can make an agent leak customer data, and most organisations can't see it happening.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Gateway that checks every agent action, refuses what breaks the rules and holds risky actions for a person	→ **Agents get work done without going off-script.**
Prompt-injection detector trained in-house; poisoned documents and memory removed or withheld	→ **Attacks hidden in content are stopped before they act.**
Tax file numbers, API keys and sensitive data blocked or redacted; bulk requests refused	→ **Sensitive data stays inside.**
Shadow AI discovery finds unsanctioned AI tools	→ **You know which AI is really in use.**
Playbooks, tool kill switch and automatic containment; SIEM content for Splunk and Sentinel	→ **Incidents are contained automatically and fit your existing SOC.**
Live Attack View and a tamper-evident record of every decision	→ **You can show exactly what each agent did and why.**
Proven under published attack simulations (Atomic Red Team, mapped to MITRE ATT&CK and ATLAS): network zones that refuse by default, its own certificate authority for encrypted links, staff logins with MFA, alerts sent to a SIEM	→ **Defences tested the way an attacker would test them.**
Microsoft 365 connect with phishing quarantine; feeds evidence into readiness reports	→ **Guardian protects and proves compliance at the same time.**

IN PRACTICE

A support agent built on a large language model receives an email hiding an instruction to export customer records. Guardian recognises the injected instruction, refuses the bulk export, raises an incident and records the decision, while the agent keeps answering normal requests.

OUTCOME
Adopt AI agents with confidence

OUTCOME
Data leaks stopped at the source

OUTCOME
Evidence of AI control for auditors

WHO IT IS FOR

Organisations deploying AI agents or copilots

SEE IT FOR YOURSELF

Sample console: guardian.cybersentien.com/console

Govern every AI system, from the register to the regulator

THE CHALLENGE

New AI laws and standards are arriving fast. Most organisations don't know every AI system in use, let alone whether each one has been assessed.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
AI register with owner, purpose and risk tier; unregistered AI found and flagged	→ **A complete inventory of the AI you use.**
Request and approval workflow with the risk tier in front of the approver	→ **Staff ask, approvers decide quickly, and every decision is recorded.**
Impact assessments, bias screening (four-fifths rule) and drift monitoring	→ **High-risk AI is checked before and after go-live.**
EU AI Act toolkit: classification, Article 73 incident clock, Article 4 literacy records, Annex IV technical file	→ **EU obligations handled step by step.**
ISO/IEC 42001 Statement of Applicability and an AI policy drafted from your own register	→ **Ready for certification preparation.**
Reported against ISO/IEC 42001, the EU AI Act, the NIST AI RMF and more AI frameworks	→ **One evidence base for every AI rule you face.**

IN PRACTICE

A department wants to use a new AI tool. The request arrives with its risk tier; the approver sees the impact assessment status before deciding. The decision is recorded, the AI register updates, and the ISO/IEC 42001 and EU AI Act evidence follows automatically.

OUTCOME
Full visibility of AI use

OUTCOME
Faster, safer AI approvals

OUTCOME
Readiness for AI regulation

WHO IT IS FOR
Boards, risk teams, AI leads and public-sector agencies

SEE IT FOR YOURSELF
AI governance in the live demo

Interviews that become evidence, automatically

THE CHALLENGE

Assessment interviews create pages of notes that someone has to type up, check and file. Valuable answers are often lost or can't be proven later.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Browser-to-browser video calls hosted by the engine itself, no Zoom or Teams needed	→ **Meet clients inside the assessment, with nothing to install.**
Every person gives permission before anything is recorded	→ **Consent is clear and recorded.**
Each browser records its own microphone, so speaker labels are facts	→ **You know exactly who said what.**
Calls transcribed and written up as notes on CyberSentien's own AI, on your server	→ **Notes are ready soon after the call, and stay private.**
The assessor accepts or rejects each note; accepted notes go straight into evidence, sealed	→ **Interview answers count as evidence without retyping.**
Recordings encrypted under the organisation's key, kept 30 days	→ **Sensitive conversations are protected.**

IN PRACTICE

An assessor interviews the IT manager on a video call inside CyberSentien. Both agree to recording. Afterwards the transcript is written up as notes; the assessor accepts the ones that answer controls, and they are saved to the client's evidence, sealed, with no retyping.

OUTCOME
No more typing up interview notes

OUTCOME
Answers captured as evidence

OUTCOME
Shorter assessments

WHO IT IS FOR
Assessors, consultants and internal audit teams

SEE IT FOR YOURSELF
Video calls in the live demo

Answer security questionnaires from your own evidence

THE CHALLENGE

Sales teams wait on security teams to answer long customer questionnaires. Each one takes days and the answers drift from one customer to the next.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Security questionnaires answered from your evidence, each answer cited	→ **Questionnaires turn around fast and consistently.**
Unsure answers are marked for a person	→ **Every answer you send is one you can stand behind.**
Per-organisation trust centre built only from verified controls	→ **Customers can see your security posture on demand.**
Shared only when you switch it on, with expiring share links	→ **You decide who sees what, and for how long.**

IN PRACTICE

A prospect sends a 200-question security questionnaire. The team answers it from its own evidence, with each answer cited; the few uncertain items go to the security lead. The prospect is also given a link to the trust centre, which shows only verified controls.

OUTCOME
Deals move faster

OUTCOME
Security team time handed back

OUTCOME
Consistent answers every time

WHO IT IS FOR
SaaS vendors, suppliers and sales teams

SEE IT FOR YOURSELF
Trust centre in the demo

Serve more clients without more hours

THE CHALLENGE

Consultancies and MSSPs grow by adding people, because each client means more evidence chasing, more reports and more context switching.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Consultant console that switches between clients, each in its own isolated workspace	→ **Work across many clients with no data crossing.**
Working papers with author, time, scope and evidence on every note	→ **Your files are audit-quality by default.**
Managed-client meter for per-client billing	→ **Bill accurately for the service you deliver.**
MSSP/MDR readiness framework	→ **Prove your own service meets the standard clients expect.**
Partner programme: no upfront cost, revenue share for consultants, introducers and resellers	→ **Grow revenue with CyberSentien at no upfront cost.**
Partner invite links open a full, unwatermarked trial	→ **Show prospects the real thing.**

IN PRACTICE

A consultant manages several clients from one console, switching between isolated workspaces. Working papers record author, time and evidence for every note, and the managed-client meter supports accurate billing for each client.

OUTCOME
More clients per consultant

OUTCOME
Higher-quality deliverables

OUTCOME
New recurring revenue

WHO IT IS FOR
Consultants, audit practices, MSPs and MSSPs

SEE IT FOR YOURSELF
Partner programme: ask for an invite link

The right expert, matched to your gaps

THE CHALLENGE

When a gap needs a person, finding a credible, independent expert takes weeks of calls, and it's hard to know whose credentials are real.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Independent CISSP, CISM, IRAP, PCI QSA, ISO lead auditor, pen-test and vCISO experts	→ **Specialist help for every kind of gap.**
Credentials checked against the issuing body's public register: "Verified" or "Self-declared"	→ **You know whose credentials are confirmed.**
A free gap check matches each organisation to experts for its own gaps	→ **You meet experts who fit your needs, not a generic list.**
Introductions only with consent	→ **Contact on your terms.**
A re-run of the engine proves when a gap is closed; reviews only from booked work	→ **You can judge experts on results, not marketing.**

IN PRACTICE

A free gap check shows an organisation needs help with PCI DSS. The directory suggests independent QSAs whose credentials are verified against the public register. After the work, a re-run of the engine shows the gap closed, and the review is tied to that booked job.

OUTCOME
The right help, fast

OUTCOME
Credentials you can trust

OUTCOME
Proof that the work closed the gap

WHO IT IS FOR
Organisations needing hands-on help; independent experts wanting clients

SEE IT FOR YOURSELF
demo.cybersentien.com/experts

Evidence and reports no one can quietly change

THE CHALLENGE

Auditors, regulators and courts ask a simple question: how do you know this file wasn't changed? Most tools can't answer it.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Every report, answer, assessment, export, upload and supplier record fingerprinted (SHA-256) into one blockchain-style hash chain	→ **Any later change is detectable.**
Signed checkpoints, time-stamped by independent public timestamp authorities (RFC 3161)	→ **Proof of when, from parties outside CyberSentien.**
QR code and seal ID on every PDF page	→ **Anyone holding a report can check it.**
Offline checker and an append-only audit log of every change	→ **Verification works even without CyberSentien.**
Connector credentials encrypted in a vault; versioned encrypted backups with restore checks	→ **The platform protecting your evidence is itself protected.**

IN PRACTICE

A regulator asks for the assessment report from last year. The organisation provides the PDF; the regulator scans the QR code and checks the seal against the ledger, proving the report is exactly what was issued on that date.

OUTCOME
Evidence that stands up in an audit or dispute

OUTCOME
Trust from regulators and customers

OUTCOME
A full history of every change

WHO IT IS FOR
Regulated organisations, assessors and legal teams

SEE IT FOR YOURSELF
Verify a sealed report from its QR code

Your evidence stays in your hands

THE CHALLENGE

Many compliance platforms ask you to upload your most sensitive security evidence to someone else's cloud. For regulated organisations that is a risk in itself.

WHAT CYBERSENTIEN DOES	WHAT IT MEANS FOR YOU
Production runs on your own server or cloud, set up in a few easy steps with an install pack and launchers for Windows, macOS and Linux	→ **Choose infrastructure that suits you; it's yours, so you stay in full control.**
CyberSentien's proprietary AI, tuned in-house, runs on the same infrastructure	→ **Your evidence stays private to you, away from public AI services.**
CPU mode on an ordinary server, or GPU mode on your own card (24 GB minimum, 48 GB recommended)	→ **Start on hardware you already have and scale when you need to.**
One evidence spine: connectors, documents and assessor decisions resolve to one control status	→ **Every screen and report tells the same story.**
Each organisation is its own isolated workspace	→ **Consultants and MSSPs serve many clients safely.**
14-day trials hosted on CyberSentien's Australian server; trial data deleted at the end	→ **Try it quickly, then move to your own environment.**

IN PRACTICE

An organisation installs CyberSentien on its own cloud account using the install pack. Connectors run inside that environment, the AI runs on the same server, and evidence stays within the organisation's own security boundary.

OUTCOME
Data sovereignty by design

OUTCOME
Simple installation

OUTCOME
Fits your security policies

WHO IT IS FOR
CIOs, CISOs, architects and procurement

SEE IT FOR YOURSELF
Deployment guide on request

WHO IT SERVES

Built for each sector's own rules

Banks, insurers and super funds

APRA CPS 234, CPS 230 and CPS 220, with CPS 230 registers; PCI DSS, CDR, fraud and AML.

Mortgage and credit brokers

NCCP Act credit licensee obligations and the mortgage broker best interests duty, plus privacy.

Government and defence

ISM / IRAP, ASD Essentials, Essential Eight, PSPF, DISP, Hosting Certification Framework, RFFR, CMMC, FedRAMP and the government AI policies.

Critical infrastructure, rail and OT

SOCI risk management program, IEC 62443 (3-2, 3-3, 4-2) and CLC/TS 50701 for rail, with OT zone reports.

Healthcare

HIPAA Security, Breach Notification and Privacy Rules, PHIPA (Ontario), HITRUST CSF and the Australian Privacy Principles.

Schools and early childhood

Australian Schools Assurance and Early Childhood Education and Care packs, with child-safe privacy and breach reporting.

Small business

SMB1001, Cyber Essentials and ASD Essentials, with simple tiles and a Supplier Pack for proving compliance to larger customers.

Retail

Its own Retail Command Centre; Retail Resilience checklists for help-desk resets, customer and loyalty logins, ransomware payment reporting and facial recognition; and a Guardian retail pack against refund and gift-card fraud by AI agents.

Technology, SaaS and AI vendors

SOC 1, 2 and 3, ISO 27001, 27017, 27018, 27034 and 42001, the EU AI Act and NIST AI RMF, with Guardian for AI agents.

Consultants, practices and MSSPs

Multi-client console, working papers, managed-client billing, the MSSP/MDR readiness framework and the partner programme.

Any organisation with suppliers

Third-party risk management, supplier questionnaires and board reporting.

International

United Kingdom (NCSC CAF, UK GDPR, Data Protection Act 2018, Cyber Essentials), New Zealand (NZISM, Privacy Act 2020), Canada (PIPEDA, PHIPA), United States (NIST, HIPAA, FedRAMP, CMMC, OMB), the EU, and coming soon the Middle East and Türkiye (Saudi NCA ECC and SAMA, UAE, ADGM, DIFC, Qatar, Bahrain, Jordan, Egypt, Israel, KVKK).

ALSO INCLUDED

The depth underneath

OT and rail

- IEC 62443 zone, conduit and security-level model: each zone carries its own obligations, so an SL-T 3 zone is never scored like an SL-T 1 zone
- Threat model laid over the system assessment boundary
- OT zone reports, rail assurance reports and incident management briefings

Government AI assurance

- NSW AI Assessment Framework submission: the 465-question pack with draft answers built from your evidence
- AI use-case register, impact assessment and transparency statement generator
- Public-sector accountability pack and procurement vendor checks

Obligations and regulation

- Legal, regulatory and contractual obligations kept as their own records, linked to the controls that meet them
- Each obligation shows where it is in force
- Regulation texts held as citable passages for Ask and the advisor
- Assurance graph: organisation, obligation, control, evidence, finding and risk joined in one view
- Secure design principles checklist read from live evidence

Platform trust

- The engine's own software bill of materials (SBOM)
- Append-only, hash-chained audit log of every change, per organisation
- Connector credentials encrypted at rest in a secret vault
- Versioned encrypted backups with automated restore checks
- Organisation export and deletion that finds everything an organisation owns before it copies or removes it

Install and licensing

- Self-install pack and licence key delivered automatically after purchase, so a customer can install on their own server with nobody from CyberSentien involved
- Upgrade from demo to a paid plan without leaving the console

On the website

- Control guides for every framework in the catalogue
- A calculator for the time and money a team could get back
- Expert directory and free demo, open to anyone

FRAMEWORK CATALOGUE

76 frameworks live, 14 coming soon

Every framework below is live except the group marked "Coming soon". Pick one or many: the same evidence is read once and answers each framework you choose. When a framework publishes a new edition, the newest becomes the default and the previous edition stays selectable.

Cyber security and information security 20

- ISO/IEC 27001
- SOC 2 Trust Services Criteria
- SOC 1
- SOC 3
- NIST Cybersecurity Framework 2.0
- NIST SP 800-53 Rev 5
- CIS Controls v8
- HITRUST CSF Readiness
- FedRAMP Rev 5
- CMMC Level 2 readiness (NIST SP 800-171 aligned)
- ISO/IEC 27017-aligned assessment
- ISO/IEC 27018-aligned assessment
- ISO/IEC 27034-aligned assessment
- ISO/IEC 27036-aligned assessment
- secure software development lifecycle gates
- CISSP-aligned eight-domain advisory
- SMB1001:2026 Readiness
- CISA Zero Trust Maturity Model
- CIS Microsoft Azure Foundations
- CIS Google Cloud Platform Foundation

Australian government and defence 7

- Information Security Manual / IRAP
- ASD Essentials for enterprise IT
- Essential Eight (ASD)
- Protective Security Policy Framework (Release 2026)
- Defence Industry Security Program (DISP) readiness
- Hosting Certification Framework (HCF) readiness
- Right Fit For Risk cyber security accreditation (DEWR)

Financial services and APRA 8

- APRA CPS 234 Information Security
- APRA CPS 230 Operational Risk Management
- APRA CPS 220 Risk Management
- PCI DSS v4.0.1
- Consumer Data Right — CDR Rules, Schedule 2
- Fraud Detection and AML Assurance
- NCCP Act: credit licensee obligations
- NCCP Act: mortgage broker best interests duty

Privacy, breach and health 5

- Australian Privacy Principles (Privacy Act 1988, Schedule 1)
- Australian Breach Reporting
- HIPAA Security, Breach Notification and Privacy Rules
- PIPEDA (Canada)
- PHIPA (Ontario) health information

Critical infrastructure, OT and rail 5

- SOCI Critical Infrastructure Risk Management Program
- IEC 62443-3-2-aligned OT Risk Assessment
- IEC 62443-3-3-aligned OT System Security Assessment
- IEC 62443-4-2-aligned OT Component Security Assessment
- CLC/TS 50701-aligned Railway Cybersecurity Assessment

United Kingdom and New Zealand 6

- NCSC Cyber Assessment Framework (CAF) v4.0 (UK)
- Cyber Essentials v3.3 (UK)
- UK General Data Protection Regulation (UK GDPR)
- UK Data Protection Act 2018
- New Zealand Information Security Manual (NZISM) v3.9
- Privacy Act 2020 (New Zealand)

Sector packs 6

- Managed Security Service Provider (MSSP/MDR) readiness
- Australian Schools Assurance
- Australian Early Childhood Education and Care
- Retail Resilience (AU)
- Third-Party Risk Management
- Environmental and Sustainability Readiness

AI governance (Australia and international) 19

- CyberSentien AI Governance Assurance
- ISO/IEC 42001
- European Union AI Act
- NIST AI Risk Management Framework
- NIST AI 600-1 Generative AI Profile
- Australia's AI Ethics Principles
- Policy for the Responsible Use of AI in Government
- National Framework for Assurance of AI in Government
- NSW AI Assessment Framework
- NSW Generative AI and AI Agent Guidance
- Queensland FAIRA Framework
- Tasmanian Government AI Guidance
- OECD AI Principles
- UNESCO Recommendation on the Ethics of AI
- United Nations General Assembly Resolution 78/265
- UAE AI Ethics Guide
- India AI Governance Guidelines
- US OMB M-25-21
- US OMB M-25-22

Coming soon COMING SOON 14

- Saudi Arabia NCA Essential Cybersecurity Controls (ECC)
- SAMA Cyber Security Framework (Saudi Arabia)
- Saudi Arabia Personal Data Protection Law
- UAE Federal Personal Data Protection Law (Decree-Law 45/2021)
- ADGM Data Protection Regulations (Abu Dhabi)
- DIFC Data Protection Law (Dubai)
- Qatar Personal Data Privacy Protection Law
- Central Bank of Bahrain cyber security requirements
- Bahrain Personal Data Protection Law
- Jordan Personal Data Protection Law
- Egypt Personal Data Protection Law (Law 151/2020)
- Israel Privacy Protection (Data Security) Regulations 2017
- Türkiye Personal Data Protection Law (KVKK, Law 6698)
- ISO/IEC 27090 AI security

CIS Benchmark library: 342 benchmarks COMING SOON

Operating systems, cloud, containers, databases, browsers, network devices and applications, each read with CyberSentien's own statements over the CIS recommendation numbers and short titles.

AKS Optimized Azure Linux 2
AKS Optimized Azure Linux 3
Alibaba Cloud Foundation
Alibaba Cloud Linux 3
AlmaLinux OS 10
AlmaLinux OS 8
AlmaLinux OS 9
Amazon Elastic Kubernetes Service (EKS)
Amazon Elastic Kubernetes Service (EKS) Auto Mode
Amazon Linux 2
Amazon Linux 2 STIG
Amazon Linux 2014.09
Amazon Linux 2023
Amazon Linux 2023 STIG
Amazon Web Services Foundations
Apache Cassandra 4.0
Apache Cassandra 4.1
Apache Cassandra 5.0
Apache HTTP Server 2.4
Apache Server 2.4 Windows STIG
Apache Tomcat 10.1
Apache Tomcat 7
Apache Tomcat 8
Apache Tomcat 9
Apache Tomcat Application Server 9 STIG
Apple iOS 18 and iPadOS 18 Intune
Apple iOS 26
Apple iOS 26 and iPadOS 26 Intune
Apple iOS iPadOS 18 STIG
Apple iPadOS 26
Apple macOS 12.0 Monterey
Apple macOS 12.0 Monterey Cloud-tailored
Apple macOS 13.0 Ventura
Apple macOS 13.0 Ventura Cloud-tailored
Apple macOS 14 (Sonoma) STIG
Apple macOS 14.0 Sonoma
Apple MacOS 14.0 Sonoma Intune
Apple macOS 15 (Sequoia) STIG
Apple macOS 15.0 Sequoia
Apple macOS 15.0 Sequoia Cloud-tailored
Apple MacOS 15.0 Sequoia Intune
Apple macOS 26 Tahoe
Apple MacOS 26 Tahoe Intune
Apple macOS 26 Tahoe STIG
Apple macOS 27 Golden Gate
Arista EOS
Arista MLS EOS 4.X L2S STIG
Arista MLS EOS 4.X NDM STIG
Arista MLS EOS 4.X Router STIG
AWS Compute Services
AWS Database Services
AWS End User Compute Services
AWS Storage Services
Azure Container Linux
Azure Kubernetes Service (AKS)
Azure Kubernetes Service Automatic (AKS Automatic)
Azure Linux 4
BIND 9.x STIG
BottleRocket
Check Point Firewall
Cisco ACI Layer 2 Switch STIG
Cisco ACI NDM STIG
Cisco ACI Router STIG
Cisco ASA 9.x Firewall
Cisco Firepower Threat Defense
Cisco Firewall
Cisco IOS Router NDM STIG
Cisco IOS Router RTR STIG
Cisco IOS Switch L2S STIG
Cisco IOS Switch NDM STIG
Cisco IOS Switch RTR STIG
Cisco IOS XE 16.x
Cisco IOS XE 17.x
Cisco IOS XE Router RTR STIG
Cisco IOS XE Switch L2S STIG
Cisco IOS XE Switch RTR STIG
Cisco IOS XR 7.x
Cisco NX OS Switch L2S STIG
Cisco NX OS Switch NDM STIG
Cisco NX OS Switch RTR STIG
Cisco NX-OS
Cloud Linux AlmaLinux OS 9 STIG
CockroachDB v25.x
Debian Linux 11
Debian Linux 11 STIG
Debian Linux 12
Debian Linux 13
DigitalOcean Foundations
DigitalOcean Services
Docker
Dragos Platform 2.x STIG
Everpure FlashArray Purity 6.9.x
Everpure FlashBlade Purity 4.5.x
ExtremeNetworks SLX-OS-20.X.X
Forescout Network Access Control STIG
Forescout Network Device Management STIG
Fortigate 7.0.x
FortiGate 7.4.x
FreeBSD 14
GitHub
GitLab
Google Android
Google Android 13 COBO STIG
Google Android 13 COPE STIG
Google Android 14 COBO STIG
Google Android 14 COPE STIG
Google Android 15 COBO STIG
Google Android 15 COPE STIG
Google Chrome
Google Chrome Browser Cloud Management
Google Chrome Enterprise Core Browser
Google Chrome Group Policy
Google ChromeOS
Google Container-Optimized OS
Google Kubernetes Engine (GKE)
Google Kubernetes Engine (GKE) Autopilot
Google Workspace Foundations
Honeywell Android 13 COBO STIG
Honeywell Android 13 COPE STIG
HPE Aruba Networking CX Switch
IBM AIX 7
IBM CICS Transaction Server 6.1
IBM Cloud Foundations
IBM Db2 11
IBM Db2 12.1
IBM Db2 13 for z OS
IBM i V7R4M0
IBM i V7R5M0
IBM WebSphere Liberty
IBM WebSphere Liberty Server STIG
IBM z OS ACF2 STIG
IBM z OS RACF STIG
IBM z OS TSS STIG
IBM z OS V2R5 with RACF
IBM z OS with RACF
IBM zSecure Suite STIG
Infoblox 8.x DNS STIG
Juniper OS
Juniper Router NDM STIG
Juniper Router RTR STIG
Juniper SRX Services Gateway ALG STIG
Juniper SRX Services Gateway VPN STIG
Juniper SRX SG IDPS STIG
Juniper SRX SG NDM STIG
Kubernetes
Kubernetes STIG
Linux Mint 22
MariaDB 10.11
MariaDB 10.6
MariaDB Enterprise 10.x STIG
MCP Server
Microsoft 365 Foundations
Microsoft Azure Compute Services
Microsoft Azure Database Services
Microsoft Azure Storage Services
Microsoft Defender Antivirus
Microsoft DotNet Framework 4.0 STIG
Microsoft Dynamics 365 Power Platform
Microsoft Edge
Microsoft Entra ID STIG
Microsoft Exchange 2016 Edge Transport Server STIG
Microsoft Exchange 2016 Mailbox Server STIG
Microsoft Exchange 2019 Edge Server STIG
Microsoft Exchange 2019 Mailbox Server STIG
Microsoft Exchange Server 2013
Microsoft Exchange Server 2016
Microsoft Exchange Server 2019
Microsoft IIS 10
Microsoft IIS 8
Microsoft Intune for Apple iOS 17 and iPadOS 17
Microsoft Intune for Edge
Microsoft Intune for Microsoft Defender Antivirus
Microsoft Intune for Office
Microsoft Intune for Windows 10
Microsoft Intune for Windows 11
Microsoft Intune MDM Service Desktop & Mobile STIG
Microsoft Office 365 ProPlus STIG
Microsoft Office Enterprise
Microsoft Office Excel 2016
Microsoft Office System 2016 STIG
Microsoft SQL Server 2012
Microsoft SQL Server 2012 Database Engine
Microsoft SQL Server 2014
Microsoft SQL Server 2019
Microsoft SQL Server 2022
Microsoft SQL Server 2022 Database STIG
Microsoft SQL Server 2022 Instance STIG
Microsoft SQL Server 2025
Microsoft Windows 10 EMS Gateway
Microsoft Windows 10 Enterprise
Microsoft Windows 10 Enterprise Release 1511
Microsoft Windows 10 Enterprise Release 1607
Microsoft Windows 10 Enterprise Release 1703
Microsoft Windows 10 Enterprise RTM Release 1507
Microsoft Windows 10 Stand-alone
Microsoft Windows 10 STIG
Microsoft Windows 11 Enterprise
Microsoft Windows 11 Stand-alone
Microsoft Windows 11 STIG
Microsoft Windows Server 2008 non-R2
Microsoft Windows Server 2012 non-R2
Microsoft Windows Server 2012 R2
Microsoft Windows Server 2016
Microsoft Windows Server 2016 STIG
Microsoft Windows Server 2019
Microsoft Windows Server 2019 Stand-alone
Microsoft Windows Server 2019 STIG
Microsoft Windows Server 2022
Microsoft Windows Server 2022 Stand-alone
Microsoft Windows Server 2022 STIG
Microsoft Windows Server 2025
Microsoft Windows Server 2025 Stand-alone
Microsoft Windows Server 2025 STIG
Microsoft Windows Server Domain Name System (DNS) STIG
MongoDB 5
Mongodb 6
MongoDB 7
MongoDB 8
Motorola Solutions Android 13 COBO STIG
Motorola Solutions Android 13 COPE STIG
Mozilla Firefox ESR GPO
Mozilla Firefox STIG
MS SQL Server 2016 Database STIG
MS SQL Server 2016 Instance STIG
NGINX
OceanBase Enterprise Edition V4
Okta Identity as a Service (IDaaS) STIG
OPNsense
Oracle Cloud Infrastructure Container Engine for Kubernetes(OKE)
Oracle Cloud Infrastructure Foundations
Oracle Database 12c STIG
Oracle Database 19c
Oracle Database 23ai
Oracle Database 26ai
Oracle Linux 10
Oracle Linux 7 STIG
Oracle Linux 8
Oracle Linux 8 STIG
Oracle Linux 9
Oracle MySQL Community Server 8.4
Oracle MySQL Community Server 9.7
Oracle MySQL Enterprise Edition 8.0
Oracle MySQL Enterprise Edition 8.4
Oracle MySQL Enterprise Edition 9.7
Oracle SaaS Cloud Applications
Oracle Solaris 11.4
Palo Alto Firewall 10
Palo Alto Firewall 11
Palo Alto Networks ALG STIG
Palo Alto Networks IDPS STIG
Palo Alto Networks NDM STIG
Palo Alto Networks Prisma Cloud Compute STIG
pfSense Firewall
PostgreSQL 13
PostgreSQL 14
PostgreSQL 15
PostgreSQL 16
PostgreSQL 17
PostgreSQL 18
Red Hat Enterprise Linux 10
Red Hat Enterprise Linux 10 STIG
Red Hat Enterprise Linux 8
Red Hat Enterprise Linux 8 STIG
Red Hat Enterprise Linux 9
Red Hat Enterprise Linux 9 STIG
Red Hat OpenShift Container Platform
Redhat OpenShift Virtual Machine Extension
RHEL8 on IBM Z Linux
Rocky Linux 10
Rocky Linux 8
Rocky Linux 9
Samsung Android 15 BYOAD STIG
Samsung Android OS 13 with Knox 3.x COBO STIG
Samsung Android OS 13 with Knox 3.x COPE STIG
Samsung Android OS 14 with Knox 3.x STIG
Samsung Android OS 15 with Knox 3.x COBO STIG
Samsung Android OS 15 with Knox 3.x COPE STIG
SingleStore 8
Snowflake Foundations
Solaris 11 SPARC STIG
Solaris 11 X86 STIG
Sophos Firewall v21
Sophos Firewall v22
SUSE Linux Enterprise 11
SUSE Linux Enterprise 12
SUSE Linux Enterprise 15
SUSE Linux Enterprise 16
SUSE Linux Enterprise Server 15 STIG
Talos Linux
Tanium 7.x Application on TanOS STIG
Tanium 7.x Operating System on TanOS STIG
Tanium 7.x STIG
Tencent Cloud Enterprise Foundation
Tencent Cloud Foundation
Tencent TDSQL 10.3.22
TencentOS Linux 4
Ubuntu Linux 18.04 LTS
Ubuntu Linux 20.04 LTS
Ubuntu Linux 20.04 LTS STIG
Ubuntu Linux 22.04 LTS
Ubuntu Linux 22.04 LTS STIG
Ubuntu Linux 24.04 LTS
Ubuntu Linux 24.04 LTS STIG
Ubuntu Linux 26.04 LTS
Versa OS Ubuntu 18.04 LTS
Versa OS Ubuntu 22.04 LTS
Visual Studio Code GPO
VMWare ESXi 7
VMware ESXi 8.0
VMware ESXi 9.0
VMware NSX 4.x Distributed Firewall STIG
VMware NSX 4.x Manager NDM STIG
VMware NSX 4.x Tier-0 Gateway Firewall STIG
VMware NSX 4.x Tier-0 Gateway Router STIG
VMware NSX 4.x Tier-1 Gateway Firewall STIG
VMware NSX 4.x Tier-1 Gateway Router STIG
VMware vSphere 7.0 ESXi STIG
VMware vSphere 7.0 VAMI STIG
VMware vSphere 7.0 vCenter Appliance EAM STIG
VMware vSphere 7.0 vCenter Appliance Lookup Service STIG
VMware vSphere 7.0 vCenter Appliance Perfcharts STIG
VMware vSphere 7.0 vCenter Appliance Photon OS STIG
VMware vSphere 7.0 vCenter Appliance PostgreSQL STIG
VMware vSphere 7.0 vCenter Appliance RhttpProxy STIG
VMware vSphere 7.0 vCenter Appliance STS STIG
VMware vSphere 7.0 vCenter Appliance UI STIG
VMware vSphere 7.0 vCenter STIG
VMware vSphere 7.0 Virtual Machine STIG
VMware vSphere 8.0 ESXi STIG
VMware vSphere 8.0 vCenter Appliance Envoy STIG
VMware vSphere 8.0 vCenter Appliance ESX Agent Manager (EAM) STIG
VMware vSphere 8.0 vCenter Appliance Lookup Service STIG
VMware vSphere 8.0 vCenter Appliance Management Interface (VAMI) STIG
VMware vSphere 8.0 vCenter Appliance Perfcharts STIG
VMware vSphere 8.0 vCenter Appliance Photon OS 4.0 STIG
VMware vSphere 8.0 vCenter Appliance PostgreSQL STIG
VMware vSphere 8.0 vCenter Appliance Secure Token Service (STS) STIG
VMware vSphere 8.0 vCenter Appliance User Interface (UI) STIG
VMware vSphere 8.0 vCenter STIG
VMware vSphere 8.0 Virtual Machine STIG
Xylok Security Suite 20.x STIG
YugabyteDB

ON THE ROADMAP

What comes next

These are planned and not yet available. They are listed here so you know where CyberSentien is heading; none of them is part of today's product.

Cyber insurance readiness ROADMAP

Assess whether an organisation is ready for cyber insurance: the controls insurers ask about in their questionnaires, such as MFA, backups, endpoint detection, patching and incident plans, read from the evidence CyberSentien already collects, with a report for the broker or insurer.

Ticket write-back ROADMAP

Send remediation items straight into Jira and ServiceNow, so fixes are tracked where your team already works.

Slack and Microsoft Teams alerts ROADMAP

Alerts for drift, new attack paths, incidents and regulator deadlines, delivered to the channels your team watches.

Security policy writer ROADMAP

Draft security policies from your own settings and registers, extending the AI use policy drafting available today.

Dark web and leaked-credential monitoring ROADMAP

Watch for your organisation's leaked credentials and mentions outside your network, alongside the inside-out exposure register available today.

Phishing simulation and awareness campaigns ROADMAP

Run staff phishing simulations and awareness training. Today CyberSentien reads your existing training and Microsoft 365 attack-simulation results as evidence.

Penetration testing through partners

Penetration testing is delivered by qualified people. Through the expert directory, CyberSentien connects you with independent pen testers and vCISOs today, and reads their reports as evidence.

CyberSentien

Getting started

Start with the free demo on sample documents, read a finished report, then open a 14-day trial workspace on your own evidence. Consultants, introducers and resellers can join the partner programme at no upfront cost.

Live demo
demo.cybersentien.com

Sample reports and evidence pack
cybersentien.com/sample-reports.html

Guardian sample console
guardian.cybersentien.com/console

Expert directory
demo.cybersentien.com/experts

Website, correctness and contact
cybersentien.com