B2CyberSec
IT SECURITY SOLUTIONS & SERVICES

B2CyberSec - Company Profile

Stop Guessing. Start Verifying.

Independent cybersecurity experts helping regulated and high-stakes organizations move from “we think we’re secure” to “we know we are.”

B²CyberSec

01

Executive Snapshot - Security you can explain to your Board

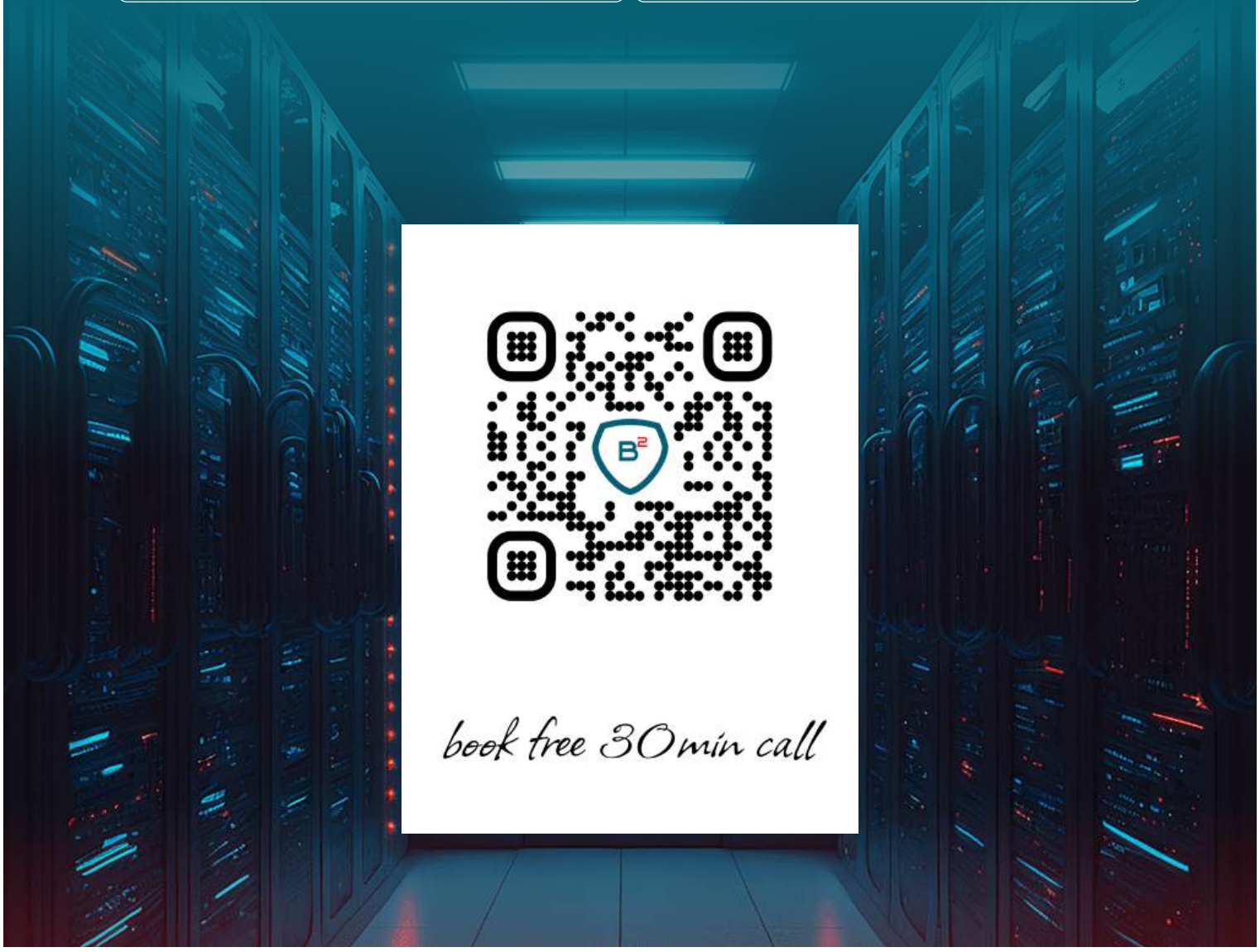
B2CyberSec GmbH is a European cybersecurity firm based in Augsburg, Germany.

We help organizations reduce cyber risk, meet regulatory requirements, and turn security into business confidence.

Our approach combines human-led penetration testing, modern security architecture, and pragmatic guidance that executives can act on.

What our clients really buy: trust, control, reliability, compliance alignment, and a competitive advantage built on demonstrable security.

Entry point: a free 30-minute risk assessment call to understand your exposure and plan the right test.



B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

02

Why B2CyberSec — From “Probably Safe” to “Proven Safe”

When cyber risk is everyone’s problem, it easily becomes no one’s priority.

Dashboards look green, tickets are closed, and months go by without visible incidents, yet attackers need only one weak identity, one misconfigured cloud bucket, one forgotten VPN tunnel. You don’t need more noise; you need an independent, outcome-driven check that converts uncertainty into a clear, defensible plan.

Independent by design.

We act as a third-party assessor with no stake in existing vendors or architectures. You get objective evidence, reproducible findings, proof of exploitation, and clear risk statements, that boards and auditors can trust.

Offense-informed defense.

We simulate real attacker behavior (not just automated scans): chaining issues across identities, network paths, apps, APIs and cloud. The result surfaces what truly matters to your business, not a long list of low-value CVEs.

Clarity for decision-makers.

Our reports translate technical findings into business impact, priorities, and cost-benefit choices. Expect an executive summary, risk scoring, attack-path visuals, and a 90-day action plan your teams can actually execute.

Compliance, without the headache.

Guidance aligned to ISO 27001, NIS2, DORA, PCI DSS and sector rules,mapped directly in the report. You’ll know what’s mandatory now, what’s recommended next, and which evidences to retain for audits.

Action to closure.

We don’t stop at the PDF. We run working sessions with your teams and providers, sequence remediation by risk/effort, and perform an optional re-test to verify fixes, so you can prove improvements, not just promise them.

What this means for you: lower exposure, fewer surprises, smoother audits, and a security story you can confidently present to customers, partners and the board.

Start with a free 30-minute risk assessment, we’ll ask targeted questions to gauge your likely exposure and recommend the right PenTest scope for your size and industry.

B²CyberSec
IT Security Solutions & Services

03

What We Do - Services That Move Risk Down

We reduce risk you can measure, not just produce paperwork.

Anyone can run a scanner and email a 100-page PDF.

We stay until the risky stuff is actually fixed.

3.1 Cyber Security & Penetration Testing

Think of us as the friendly burglars you pay to check whether your doors are really locked and which window the intern left open.

We try what real attackers try, but we leave you with the keys and a plan to upgrade the locks.

Penetration Testing (Black/Grey/White Box): Human-led simulations across external, internal, web/app, mobile, API, cloud, wireless

Red Team / Purple Team Exercises: Objective-driven, attacker-style campaigns; collaborative purple teaming to uplift detection & response.

Social Engineering: Phishing and physical security testing to validate people, process, and controls.

Vulnerability Management & Gap Analysis: From discovery to prioritization and remediation planning.

Audit Preparation: Readiness for ISO 27001, DORA, NIST frameworks, PCI DSS and more.

3.2 Network & Security Architecture

This is the building's layout and plumbing.

We redraw the floor plan so a leak in one room doesn't flood the whole house and so visitors only reach the rooms they're supposed to.

Design & Migration: SD-WAN, SD-Access, segmentation, data center & cloud connectivity.

Firewall Strategy: Next-gen firewalling, segmentation & zero trust enforcement.

Automation: Cisco & Palo Alto with Ansible / Python to scale securely.

3.3 Security Monitoring & SIEM

Our CCTV and alarm system for the digital office.

We make sure the cameras point at the right doors, the alarms don't cry wolf, and the night shift knows exactly what to do when a sensor trips.

- SIEM Implementation & Operations (e.g., Splunk) and SOC process design to improve visibility and response.

3.4 Project Leadership & Enablement

We're the steady hands with the checklist, keeping projects on track, vendors aligned, and your team learning how to fish so they're stronger next quarter.

- Project Management & Presales Architecture: Leading large-scale security initiatives end-to-end.
- Training & Workshops: Cisco/Palo Alto enablement and security awareness programs.

04

Who We Serve

We don’t try to be everything to everyone.

We take on work where we’re confident we can move the risk needle, and we say so upfront. That means clear scoping, measurable outcomes, and honest expectations.

From day one.

If we’re not the best team for your challenge, we’ll tell you early and point you in the right direction.

That’s our commitment and our transparency.

Industries: Banking & Financial Services, Public Sector, Energy & Utilities, Telecommunications, Manufacturing.

Typical profile: 250+ employees, compliance-driven, complex hybrid/ cloud environments, with gaps in internal expertise or bandwidth.

What we solve: hidden exposures, audit pressure, legacy network debt, cloud misconfigurations, weak identity & access hygiene, and limited incident visibility.

05

How We Work - Evidence Over Assumptions

We don't sell mystery or magic.

We commit to a process that reduces measurable risk, with clear scoping, transparent communication, and proof at every step.

If a test won't answer your business question, we'll say so before we start. The result is a program your board understands and your engineers can execute.

Discovery & Scoping: *no cookie-cutter tests.*

We align objectives, assets, and constraints with business priorities.

Together we define success criteria, rules of engagement, and the right approach (black/grey/white box) so the test answers the right questions, safely and efficiently.

Threat-Led Simulation: *friendly attackers, real tactics.*

Human-led testing mirrors how adversaries chain weaknesses across identities, networks, apps, APIs, and cloud.

Where relevant, we include phishing or third-party paths. Critical findings are communicated immediately, not just in the final report.

Impact-Focused Reporting: *board-ready clarity.*

Findings are mapped to CVE/CVSS, linked to attack-path visuals and real business impact. You'll get a 90-day action plan with quick wins and structural fixes, plus cost/effort guidance and compliance flags (ISO/NIS2/DORA/PCI DSS).

Guided Remediation:*we sit with your team.*

Working sessions with your engineers and providers to close gaps fast.

We prioritize by risk and effort, provide templates and acceptance criteria, and keep momentum until fixes land.

Verify & Improve: *proof, not promises.*

Optional re-test confirms closure and shows progress (risk score delta, time-to-fix, % closed).

A management debrief distills lessons learned into your roadmap.

06
Proof & Credentials

Our experts hold certifications including: CRTO, SWIFT CSP Assessor, Burp Suite Certified Practitioner, eCCPT, eJPT, CPSA, CEH, CHFI, OSCP, OSMR, PNPT.

Tooling spans best-of-breed open-source and commercial platforms; methodology aligns to OWASP, NIST, and industry good practice.

Regulatory familiarity: ISO 27001, NIS2, DORA, PCI DSS, GDPR/DSGVO, sector guidance for KRITIS and healthcare

07
Research Excellence & Certified Expertise

Our extended security network has been publicly recognized for uncovering critical vulnerabilities in widely used platforms – including iOS and Nextcloud – protecting millions of users worldwide. This research has been acknowledged by leading technology companies and government institutions, underscoring the depth of our offensive security expertise.

At the same time, our consultants are thoroughly vetted, professionally trained, and certified by international standards. From ISO 27001 and CREST to Cisco, Microsoft, and EC-Council, we ensure both technical excellence and compliance with global requirements – enabling us to operate effectively in the most regulated industries.

B²CyberSec
IT Security Solutions & Services

08

Selected Engagements — Snapshots (Anonymized)

- **Financial Services (EU):** External & cloud PenTest exposed misconfigured identity flows and an internet-reachable admin panel. Guided fix reduced attack surface and audit risk before year-end review.
- **Manufacturing (DACH):** Internal network test uncovered legacy flat network and weak service accounts; rapid segmentation plan and privileged access hardening reduced lateral-movement risk.
- **Public Sector:** API testing identified broken authorization paths; joint remedial sprints with the vendor closed high-risk gaps ahead of a public launch.

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

09

Partnership Models — Strength in Collaboration

Trustworthy by separation, effective by collaboration.

We work shoulder-to-shoulder with your internal IT and external MSPs—but we preserve independence wherever credibility and compliance require it. That means clear roles, clean handoffs, and no testing of our own implementations. You get the best of both worlds: a team that integrates smoothly while keeping the third-party objectivity auditors expect.

How we collaborate (client side):

- With internal IT / Security: day-to-day coordination, secure access, rapid triage of critical findings, and joint working sessions to land fixes fast—without disrupting operations.
- With existing MSPs / vendors: we respect established responsibilities and SLAs, share evidence, and sequence remediation so partners can execute efficiently

How we collaborate (partner side):

- Co-delivery for integrators & solution partners: structured engagement playbooks, shared RACI, and white-label options when appropriate (while keeping testing independence).
- Referral & reseller models: simple commercial frameworks to bring penetration testing into your portfolio without diluting focus.
- Enablement: templates, report samples, and pre-sales support to scope the right test and set realistic expectations with customers.

Separation of duties (non-negotiable):

For credible results and smoother audits, we do not test what we have just designed or operated. Where we contribute to architecture or operations, testing is performed by a separate B2CyberSec team or an agreed independent partner. This protects your compliance position and the value of the evidence.

Engagement hygiene you can trust:

NDA and data-handling standards, secure evidence exchange, clear communication cadences, and executive/practitioner touchpoints. Commercial models include project-based testing, framework agreements for periodic re-tests, and retainers for programmatic assurance.

10
Trusted by Global Leaders

Our extended network has collaborated with leading security providers, supported some of the world's most recognized enterprises, and contributed to research acknowledged by interna=onal ins=tu=ons.

From Google and Adobe to NATO and the US Department of Defense, our track record reflects both commercial impact and global recogni=on.

This unique combina=on of enterprise delivery and engaged research ensures that our clients benefit from exper=se tested in the most demanding environments.

Primes

VERACODE · BISHOPFOX · leviathan security group · Inspectiv · Prompt: · snyk · bugcrowd · praetorian

Contractor Experience

Google · Adobe · ZOHO · HONDA · asseco · amazon

Engaged Research

NATO OTAN · OpenAI · O'REILLY · INFOSEC INSTITUTE

11

Trusted by Global Standards

international benchmarks. From ISO and CREST to Cisco, Microsoft, EC-Council, and OffSec, our consultants meet the highest levels of recognition in the industry.

This guarantees that our delivery is not only technically excellent, but also aligned with the standards required by regulators, auditors, and enterprise clients worldwide.

Vetted, Trained, & Certified

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

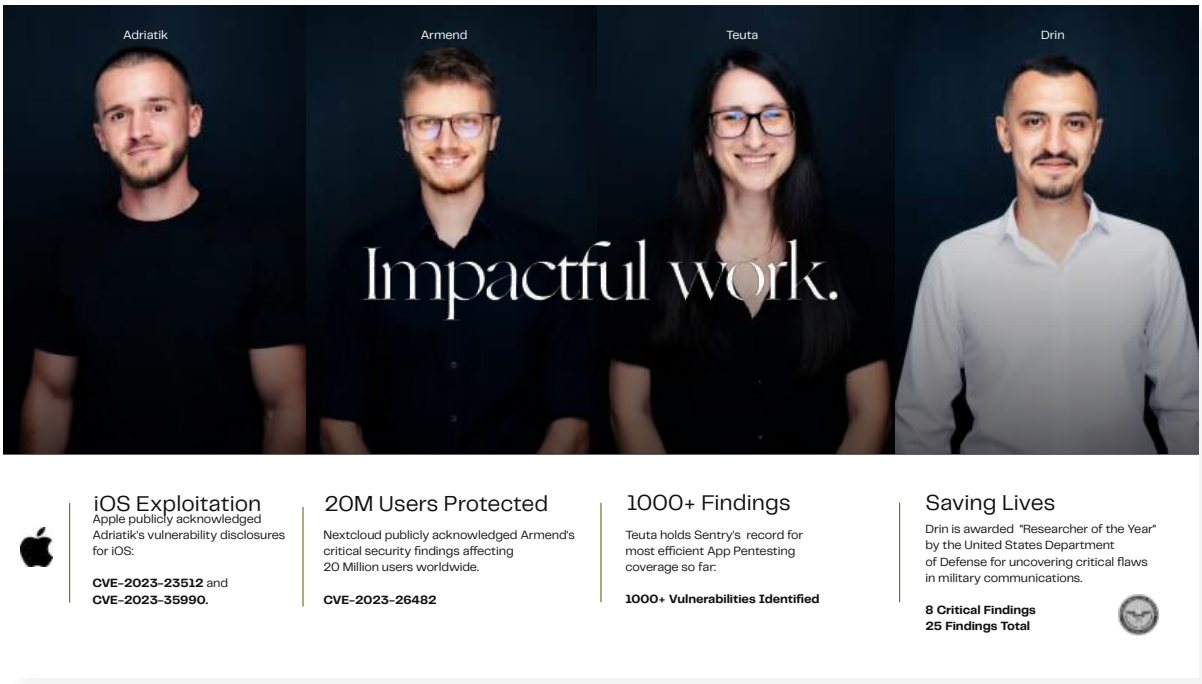
12

Impactful Research, Real-World Results

Our extended network's security research has been publicly acknowledged by leading technology companies and government institutions. From Apple and Nextcloud to the US Department of Defense, these contributions have protected millions of users and directly strengthened global security.

Highlights include:

iOS vulnerabilities disclosed and acknowledged by Apple	Critical flaws in Nextcloud securing 20M+ users worldwide	1,000+ vulnerabilities identified through advanced testing	Recognition by the US Department of Defense for saving lives in military communications



13

Leadership & Team — Specialists Who Fit Your Reality

People who can break it safely. And help you fix it fast.

We build teams the way modern security work actually happens: attacker craft paired with enterprise delivery. We take on work we believe in, commit to measurable outcomes, speak plainly, and stay engaged until changes land. No theatrics—just specialists who fit your reality and move risk down.

Cross-disciplinary depth. Engineers and consultants with deep experience across penetration testing, modern networking, cloud platforms, and security operations/SIEM. The benefit for you: findings that are technically sound and realistically remediable in complex hybrid environments.

Recognized competence. Our practitioners hold certifications including CRTO, SWIFT CSP Assessor, Burp Suite Certified Practitioner, eCCPT, eJPT, CPSA, CEH, CHFI, OSCP, OSMR, PNPT. Methods align with OWASP and NIST good practice so your evidence stands up in audits and boardrooms alike.

Senior-led, outcome-driven. Small, senior teams own the full loop—from scoping and testing to reporting and fix validation—with clear touchpoints for executives and practitioners. You always know who is doing the work and how we measure progress.

3. Public Disclosures and Research Samples

CVE-2023-25482	Insufficient user input sanitization could allow low-privileged attackers to execute arbitrary system commande in Nextcloud instances.
CVE-2023-35928	Insufficient authorization controls could allow attackers to share malicious files, thereby taking over arbitrary user accounts, including administrative ones in Nextcloud instances
CVE-2023-39960	Lack of anti-automation could allow attackers to issue brute-force passwords in the WebDAV API of the vulnerable Naxtcloud instance.
CVE-2023-23512	Improper handling of caches could allow attackers to cause Safari denial-of-service
CVE-2023-33184	Server-side Request Forgery vulnerability that cloud allow attackers to scan the internal infrastructure of the vulnerable Nextcloud instance
CVE-2023-35000	Malicious applications installed in Apple devices, could allow the identification of other installed applications within the target device.

4. Certifications

Company Certifications

- ISO 9001:2015 – Quality Management Systems
- ISO 27001:2022 – Standard for Information Security (ISMS)

Staff Certifications

- Certified AI/ML Pentester (C-AI/MLPen)
- Certified Red Team Lead (CRTL)
- Certified Red Team Operator (CRTO)
- SWIFT Customer Security Program V2023 - Expert
- Burp Suite Certified Practitioner (BSCP)
- Certified Professional Penetration Tester (eCCPT) – INE Security
- Junior Penetration Tester (eJPT) – INE Security
- CREST Practitioner Security Analyst (CPSA)
- OffSec Web Assessor (OSWA)
- OffSec Web Expert (OSWE)
- OffSec Certified Professional (OSCP)
- Cyber Academy Certified Instructor (CACI)
- Cyber Academy Certified Expert (CACE)
- Cyber Academy Certified Professional (CACP)
- Web Application Penetration Tester eXtreme (eWPTXv2)
- Mobile Application Penetration Tester (eMAPT) – INE Security
- Certified Red Team Infra Dev (CRT-ID)
- EC-Council Certified Ethical Hacker (CEH)
- EC-Council Certified Ethical Hacker Practical
- EC-Council Certified Ethical Hacker Master

Current Ongoing Certification Process:

- ISO 22301:2019 – Security and Resilience – Business Continuity Management Systems

Certifications Currently Being Pursued by Team Members:

- CREST Registered Penetration Tester (CRT)

How we lead (principles we live by):

	Independence & integrity: we tell you what you need to hear, not what tools want you to buy.
	Evidence over opinions: reproducible findings, proof of exploitation, clear risk statements.
	Clarity before complexity: plain language, visuals, and a 90-day action plan your teams can execute.
	Collaboration without disruption: we integrate with internal IT and vendors while preserving third-party objectivity.
	Measurable improvement: re-test, risk deltas, and before/after you can show to the board.

Where and how we operate. Based in Augsburg, Germany, serving DACH and Europe with English/German delivery, on-site where required and remote when efficient. We meet your security, NDA, and data-handling standards without slowing the work.

14

Proven Scale & Global Reach

As part of B2CyberSec's extended expert network, more than 2,000 penetration testing and red teaming projects have been successfully delivered for over 600 international clients across industries worldwide. This unique combination of scale and diversity provides our customers with proven expertise in web, mobile, cloud, network, API, AI, and more.

Since 2019, B2CyberSec has combined its own consulting and security expertise with this delivery power ensuring that offensive security capabilities are fully integrated into our broader consulting and CyberShield360° services.

This capability is a major pillar of our portfolio – a critical part of our mission to secure enterprises against evolving threats – but still only one part of the complete protection we provide.

2000+ Projects

Web	Mobile	Cloud	Network
API	AI	**+ more**	

600+ End Clients

Tech	Health	Finance	Media
Manufacturing	Entertainment	**+ more**	

B²CyberSec
IT SECURITY SOLUTIONS & SERVICES

15

Offensive Security – Real Attacks, Real Proof

resiliently. We uncover vulnerabilities across applications, networks, cloud, and even AI systems through realworld attack simulations – showing exactly where defenses stand, and where they need to be strengthened.

Our capabilities include:

01	02	03	04	05
Application, Mobile & Hybrid Penetration Testing	Internal & External Infrastructure Testing	Cloud Security Reviews	Operational Technology Assessments	AI Red Teaming

Each engagement is designed to replicate the tactics of real attackers – but with the control, precision, and reporting needed to turn exposures into actionable remediation.

1. Application Penetration Testing (APT)
   We help businesses protect their applications by identifying security gaps through controlled attack simulations, ensuring your software can withstand real-world threats and safeguard your users.

2. Mobile Application Penetration Testing (MAPT)
   We protect mobile users by identifying vulnerabilities in Android and\ iOS apps, ensuring sensitive data and functionality remain secure against emerging threats.

3. Internal Infrastructure Penetration Testing (IPT)
   We secure sensitive internal data by uncovering risks within networks and systems, helping organizations mitigate insider threats and unauthorized access.

4. External Infrastructure Penetration Testing (EPT)
   We help organizations protect their external IT assets by probing network perimeters, identifying weaknesses, and delivering actionable solutions to strengthen defenses against external attackers.

5. Hybrid Application Penetration Testing (HAPT)
   We provide deeper insights into application security by combining source code analysis with penetration testing, helping organizations identify and resolve vulnerabilities from development to deployment.

6. Cloud Security Review (CSR)
   We help organizations secure their cloud environments by evaluating configurations, identifying risks, and ensuring compliance with industry standards to protect sensitive data and workloads.

7. Operational Technology Penetration Testing (OTPT)
   We help secure critical industrial systems by identifying vulnerabilities in control systems and ensuring operational continuity against potential cyberattacks.

8. AI Red Teaming (AIRT)
   We help organizations secure their AI systems by simulating real-worl adversarial attacks, uncovering vulnerabilities that could compromise operations, and providing actionable strategies to enhance resilience.

16

CyberShield360° – Full-Spectrum Defensive Security

CyberShield360° is our managed security framework – combining proactive defense, continuous monitoring, and compliance support into one integrated service. It is designed to protect every layer of your business, while giving executives full visibility and confidence.

Key Components

1. vCISO (Virtual Chief Information Security Officer) Trusted leadership on demand: building, refining, and managing your security program in line with your goals and regulatory requirements.

2. MSSP (Managed Security Services) 24/7 detection, response, and neutralization of threats – ensuring uninterrupted business operations and realtime protection.

3. SOC (Security Operations Center) Continuous monitoring and incident response, with clear SLAs and reporting tailored for executives and auditors.

4. Compliance & Certification Preparation End-to-end guidance for ISO 27001, SOC 2, PCI DSS, SWIFT, HIPAA, GDPR, and DORA – ensuring your organization meets the standards that matter most.

How It Works

Integration with Offensive Security: Findings from PenTesting feed directly into CyberShield360°, so vulnerabilities don't just get reported – they get fixed and monitored.

Continuous Visibility: Dashboards and reports tailored for both technical teams and C-level management.

Scalable Coverage: From SMEs to large enterprises, CyberShield360° adapts to your risk profile and compliance needs.

1. Virtual Chief Information Security Officer (vCISO)
   We provide trusted leadership to help you build, refine, and manage a security program that supports your goals and mitigates risks.

2. Managed Security Services (MSSP)
   Our managed security services detect, respond to, and neutralize risks 24/7, so your business can operate without disruption.

3. ISO27001 Certification Preparation
   We guide you in crafting the policies and procedures needed for ISO 27001 certification, while advising on security controls to ensure compliance and achieve your certification goals.

4. Cybersecurity Certification Preparation
   We support certification preparation in achieving compliance with key cybersecurity standards, including ISO 27001, SOC 2, PCI DSS, SWIFT, HIPAA, and others.

17
Client Journey

Not every client starts in the same place. Some reach out after an expert consultation, others following a quick audit, and many as part of a larger service project. But the moment a hands-on security assessment is required, our offensive security methodology becomes part of the journey.

From this point forward, the engagement follows a clear and proven process: structured, rigorous, and transparent. Clients know what happens next, who is responsible, and when results will be delivered.

This is how we ensure that findings don't remain abstract. They are prioritized, translated into concrete actions, and tracked until resolved. The result: clarity, measurable progress, and confidence that risks are being uncovered and addressed.

Discovery Call (free) - Determine needs & maturity levels.

Expert Call (1h free) - Consultation & Recommendation Report "from ACTUAL to DESIRED state"

Quick Audit 2-5 days - Interview & remote check. Status report 5 – 10 pages (risk matrix + priorities).

Service Project - Consulting or PenTest.

CyberShield360° (SOC + MSS)

A Typical Offensive Security Project*

Every project follows three defined steps:

Scoping – tailored to the client's unique environment, risks, and objectives.

Assessment – simulating real-world attack scenarios across applications, networks, and systems.

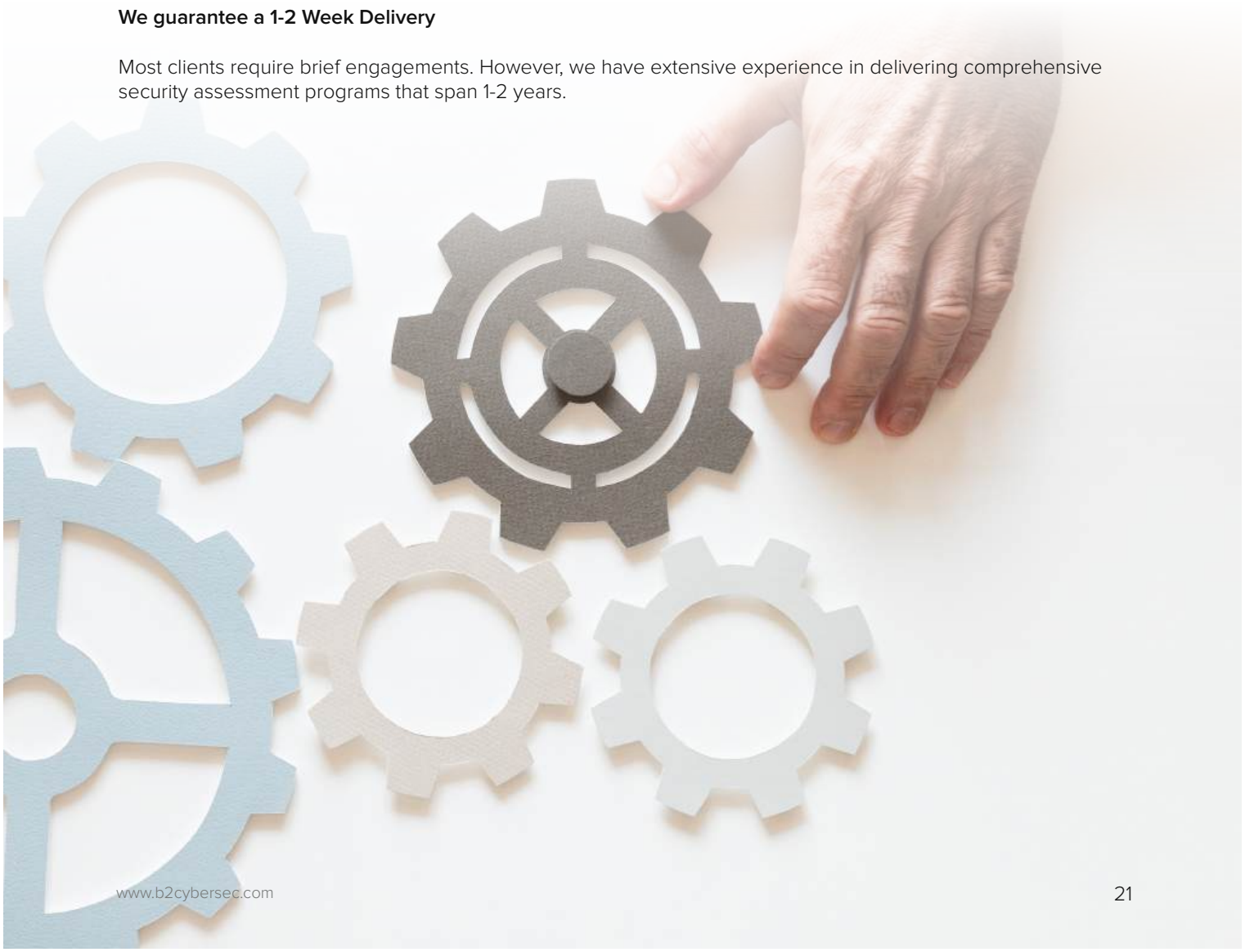
Delivery – providing clear reports, executive-ready insights, and follow-up consultations to maximize impact.

Most projects are completed within 1–2 weeks, with options for extended programs lasting up to 24 months.

White glove service with rigorous methodology.

We guarantee a 1-2 Week Delivery

Most clients require brief engagements. However, we have extensive experience in delivering comprehensive security assessment programs that span 1-2 years.



18

Dedicated Scaling Program

penetration testing, ensuring a continuous pipeline of skilled professionals. Consultants are recruited in-house from this program and trained with a strong focus on both technical expertise and client-facing delivery.

Key Benefits:

Since 2014 – over a decade of continuous operation, addressing the growing demand for cybersecurity talent.

1000+ Students – trained professionals across industries, with hands-on experience in offensive and defensive security.

700+ Labs – a massive Cyber Range with hundreds of labs designed to teach, test, and evaluate real-world skills.

Enterprise-Ready – tailored programs preparing consultants to deliver security assessments and compliance support for Fortune 500 and global organizations.

This scaling capability allows B2CyberSec to deliver projects at speed and quality, while ensuring long-term capacity for large enterprise engagements.

CYBER ACADEMY

Dedicated Scaling Program

We operate the oldest and largest vocational school for cybersecurity and penetration testing. All of our consultants are recruted in-house from the program.

Benefit #1

Since 2014

Our academy was opened in 2014 in response to a growing need for talent in the region

Benefit #2

1000+ Students

With 11+ years in operation, our academy has trained more than a thousand professionals across industries.

Benefit #3

Tailored for Sentry

The training program has tracks specially dedicated to scale for Sentry engagements, including report writing and client facing skills.

Benefit #4

Since 2014

Cyber Academy operates a massive Cyber Range with hundreds of labs designed to teach and evaluate students.

PayPal Deloitte. BNP PARIBAS

OpenAI O'REILLY INFOSEC

and more!

19

Dossier – Your Security Command Center

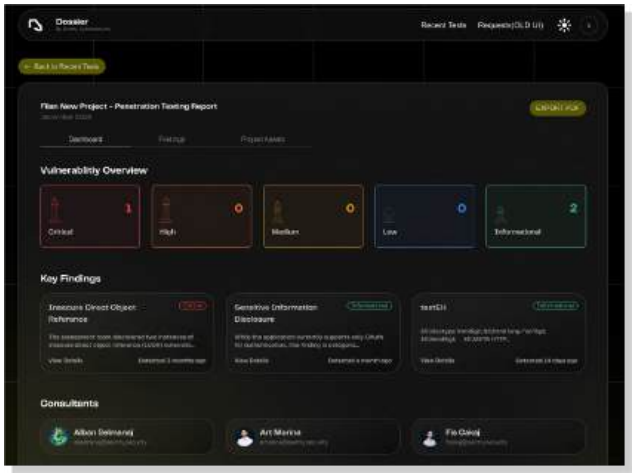
Dossier is more than a reporting portal. It's a secure AWS-based platform that manages the entire lifecycle – from the first audit or penetration test to ongoing CyberShield360° operations.

What makes it unique:

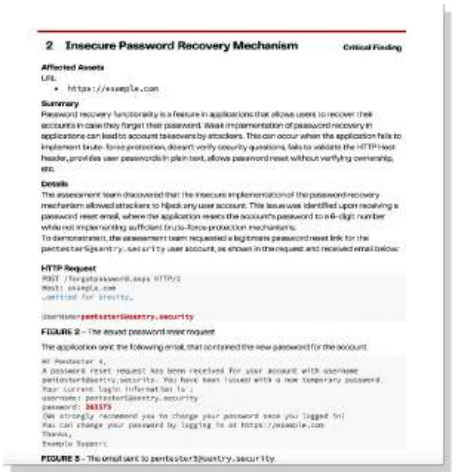
01	02	03	04	05
Centralized evidence & reports in one secure location	Real-time dashboards with remediation progress tracking	Next Steps with prioritization (urgent, high, medium, low) – so your teams know exactly what to fix first	Role-based access – tailored insights for executives, auditors, and engineers	Compliance-ready documentation for ISO 27001, NIS2, DORA, GDPR and more

With Dossier, security becomes continuous, measurable, and actionable – not just a onetime PDF report.

Compliance conscious reporting. Timely, precise, and professional.



Dossier Platform Report Variant



PDF Report Variant

Authored for executives, auditors, and technical specialists.

Our reports include insights tailored for strategic decisions, regulatory assessment, and technical remediation.

B²CYBERSEC
IT SECURITY SOLUTIONS & SERVICES

Start Here: A 30-Minute conversation that clarifies risk

Book a free 30-minute cyber risk assessment call.

We'll ask targeted questions about your environment, outline likely risk areas, and recommend the right testing approach for your size and industry.

No obligation, just clarity.

info@b2cybersec.com

+49 (0) 821 90 789 500

Werner-von-Siemens-Str. 6
86159 Augsburg, Germany

www.b2cybersec.com

book free 30min call

b2cybersec.com

B2CyberSec - We make security demonstrable.