intcube

in a nutshell

background. portfolio. innovation. team.

Content

01 Background

02 Portfolio

03 Innovation

04 Team

❯ 01 Background

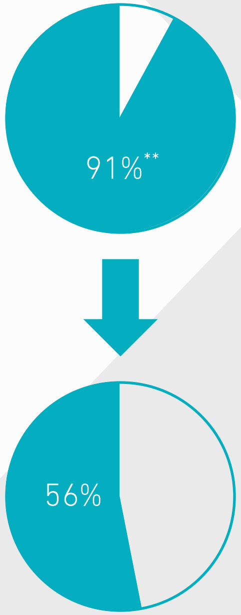
02 Portfolio

03 Innovation

04 Team

We guide mid-sized organizations to stronger cyber resilience

Companies reporting at least one cyber security incident in 2023



Thereof companies suffering moderate to severe consequences

Existential Threat*

45% of companies state that a cyber incident could threaten their very existence

Up from only 9% in 2021

Unmet Demand for Cyber Security Guidance

Mid-sized organizations...

- are the backbone of our economy and society
- struggle with digitalization
- suffer disproportionately from the war for talent
- are under constant cyber attacks

* CrowdStrike 2023 Global Threat Report

** Deloitte 2023 Global Future of Cyber survey

We exist to promote universal human values

Facts

- Founded in 2022
- HQ in Berlin
- Headcount 8+ (plan: 12HC YE2024)
- Remote first culture (w/ 3 locations)

Principles

- Purpose
- Impact
- Transparency
- Fairness

Purpose

- Strengthening cyber resilience through consulting
- Making a positive impact as a corporate citizen
- Fostering geo-cyber-economical dialogue as a Think Tank

Difference

- Promoting the goals and values of the European Union
- 25% of profits to good causes
- Full salary transparency, no gender pay gap
- Diversity is crucial for success

We implement The Unconsultancy Manifesto

We are uncovering more sustainable and reproducible ways of satisfying customers' needs for guidance and expertise.

Through this work we have come to value

- Impact over ritualized theater
- Interactions over one-way communication
- Scalability and repeatability over unnecessary individualization
- Cooperation and community building over protecting client relations
- Transparency over obscure or unfair practices

https://unconsultancy.org

We follow these principles:

1. Our highest priority is to empower our customers to make good decisions and to enable them to implement these. This we call positive impact.
2. We strive to develop approaches and build services and products that create positive impact for hundreds or thousands of organizations. This we call scale.
3. We try to maximize positive impact per effort spent. This we call impact at scale.
4. We believe that the optimal way to get there isn't always a straight line and embrace change whenever it comes. This we call adaptability.
5. We acknowledge that conflict of interests and side effects exist and try to make them visible whenever and wherever we identify them. This we call transparency.
6. Politics-free projects do not exist. Most client interactions happen at a factual, personal, and political level. Incorporating into our day-to-day work how they relate to each other and influence each other will benefit us and the client. This we call fairness.
7. Self-organized, networked organizations and engagements produce better results faster than pyramidal hierarchies. They also allow everyone involved to grow. This we call organicity.
8. "Don't be evil" isn't good enough. We are aware of potential harms of Consulting and try to counter them. This we call self-awareness.

01 Background

02 Portfolio

03 Innovation

04 Team

We provide the guidance you need

Security Projects

- Cybersecurity Strategy
- Decision-Making Support
- Solution Evaluation
- Analysis and Assessment

Long-Term Engagements

- Chief Information Security Officer (CISO)
- Information Security Officer
- IT Security Officer
- Interim Manager (CIO, CTO, CPSO)

Security Project Organization

- Project Planning
- Project Reviews
- Management of Security Projects
- Project Team Coaching

You can rely on our team‘s expertise

Compliance and Assessment Frameworks

- ISO 27001
- BSI IT-Grundschutz (Baseline Protection)
- Critical Infrastructure Security / KRITIS
- NIS2
- BAIT, VAIT, DORA
- NIST CSF, CIS Controls & Benchmarks

Security Technology and IT-Domains

- Cloud Security Posture
- Source Code Audits
- Threat Intelligence
- Vulnerability Management
- Managed Cyber Defense / SOC

Security Processes

- Detection & Reaction Processes
- Incident Response Management
- Penetration Testing Program Management
- Vulnerability Management

For global investors, we increase your portfolio's cyber resilience

Buy side
Due Dilligence

- Cyber Security DD
- Security Product DD
- Tech DD
- ESG+C(yber)

Portfolio Companies
Cyber Risk Management

- Streamlined Audits
- Benchmarks
- Threat Profiles
- Actionable Insights

Portfolio Companies
Security Program

- Roadmap Development
- Execution Support
- Investor Reporting

Cybersecurity Due Dilligence Options

Fundamentals

Best for
Companies, where IT / Tech is not part of product and who do not operate in a regulated sector.

Topics covered
Fundamental IT-security practices, cyber resilience, and basic security management.

Mappings
NIST CSF

Essential

Best for
Tech companies, Manufacturers of smart devices, companies with customers in regulated/critical infrastructure sectors.

Topics covered
Everything in “Fundamentals” plus
Extended IT security practices, BCM, supply chain, cyber resilience, governance.

OT Security, IoT Security
Cloud Security
Product Security

Mappings
NIST CSF, CIS Controls

Bespoke

Best for
Cyber Security companies and companies with extended compliance requirements.

Topics covered
individual/bespoke

Mappings
individual/bespoke

01 Background

02 Portfolio

❯ 03 Innovation

04 Team

Cohorts: innovative approach for efficient and effective improvement

Situation at mid-sized orgs

- Urgent need to transform securely (digitalization, technical debt, business transformation)
- Projects fail to deliver results in time and budget.
- Information Security and IT Security are disconnected from each other and from the business.
- Often, IT Operations is torn between run-the-company and projects.
- Information security often stuck in audit and analysis.
- Security understood as a technical appendage of IT. Technology alone will not solve the problem.

Market leads to Complications

- Many new tools flood the market. Impossible to keep up with rate of new product categories.
- Aggressive vendor marketing makes cybersecurity effectively a market for lemons.
- Internal Security is reactive only, driven by changes in tech, in business and in regulations.
- Access to knowledge is limited. Very difficult and expensive to hire and retain talent.
- External consultancies' interests are not aligned with client's interests.

Resolution is found in cohorts

- A group of companies sharing a challenge at the same point in time.
- All are working on their own challenge, in sync and timeboxed.
- Progress, results and experiences are discussed and shared in the group.
- Drawing on the knowledge of the group saves valuable time.
- Sustainable effect through alumni networking.
- Lower total cost and faster results compared to consulting.
- Methodology, content, platform, organization and orchestration provided by intcube.

Cohort Success Story
Attack Surface Management

19 mid-sized portfolio companies of a single investor working together for 2 months in one cohort on Attack Surface Reduction.

Cohort Content

External Systems

- Scan of all externally reachable systems for known vulnerabilities.
- Reporting, coaching, workshops for remediation.
- Rescan and validation of successful remediation.

Phishing Emails

- Questionnaire on implemented email security.
- Analysis of replies and recommendations for improvement.

Hacked Accounts

- Questionnaire on implemented identity & access management technologies.
- Quick Darknet check for primary email domains.
- Analysis of results and recommendations for improvement.

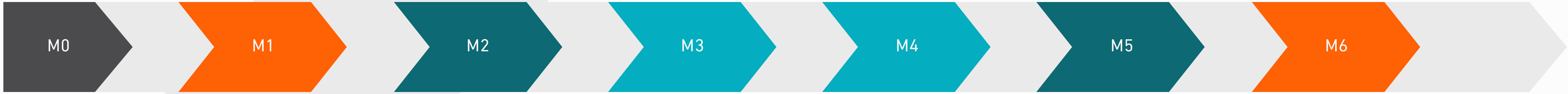
Approach, Results & Benefits

- Synchronous project in Feb/Mar 2024.
- Tooling and operations were provided centrally.
- Weekly group calls facilitated “learn from each other” and networking amongst participants.
- Fixed time & budget: Externally scheduled cadence prevented typical “project lag”.
- Invest of less than € 5.000 per entity.
- All companies remediated their critical vulnerabilities.
- Immediate, measurable risk reduction for every participant as well as further recommendations.

Cohort Example

Security Coaching and Fractional CISO

Small portfolio companies (SMEs) of a single investor being coached as a cohort and sharing a CISO



Onboarding (Month 0)

- Legal & Organizational onboarding
- Getting to know each other
- Initial assessment

Initialization (Month 1)

- Goals, Expectation, Organization
- High Value Assets & Priorities
- Alignment and synergies

Security Program Definition (Month 2)

- Shared core, individual edges
- Policies, Processes, Technologies
- Joint implementation planning.

Achieving Results (Months 3 and 4)

- Implementation of program per participant
- Leveraging synergies (same policies, same tooling)
- Weekly "progress, learned, failed, help" sessions.

Validation & Improvement (Month 5)

- Analysis of results achieved.
- Implementation of further improvements.
- Finalize documentation.

Kickdown (Month 6)

- Grace period to get things done
- Learnings, Knowledge Management
- Investor Reporting
- Follow-up activities

01 Background

02 Portfolio

03 Innovation

❯ 04 Team

Founders’ Background

Dror-John Röcher, CEO

With a degree in geophysics, Dror-John Röcher has more than 25 years of experience as a manager, coach, consultant, researcher, and penetration tester in the IT security industry. Until the end of 2021, he worked at Berlin-based DCSO Deutsche Cyber-Sicherheitsorganisation GmbH, where he was a member of the Executive Board. Prior to assuming overall revenue responsibility, Dror led DCSO's managed services as COO Cyber Defense and built DCSO's threat intelligence service, respectively. He is a recognized expert in strategic threat intelligence and in how geopolitics manifests itself in the cyber domain.

During his professional career, he has dealt with a wide range of technical and organizational information security issues and challenges. In particular, he has focused on the changes in IT security caused by digitalization as well as defense against industrial espionage and nation state threat actors. Prior to joining DCSO, he served in various principal consultant and portfolio management roles at Computacenter and as a partner at ERNW.

Dror-John Röcher regularly speaks on IT security topics at industry-relevant conferences worldwide, including Black Hat Briefings, Hack-in-the-Box, Troopers, Sector, and many more.

Founders' Background

David Fuhr, CTO

David Fuhr is a security researcher and thought leader with more than 20 years of experience in tech and security. A trained Gestalt coach, he is a well-known expert in cryptography, cloud and industrial security as well as in mathematical methods and risk modeling. With degrees in mathematics and political science and a thesis on quantum computing he has conducted applied research in artificial intelligence/machine learning (security) and knowledge management. From 2012 to 2022 he was a principal consultant and the Head of Research & Innovation at Germany's leading security boutique consultancy HiSolutions, where he coauthored several national and international security standards and built & led the innovation matrix org. During his tenure, he helped advance the security programs of more than 100 organizations.

David was the owner and founder of NTITY advanced security consultancy, the founder of DHF Polska penetration testing sourcing services, a former avid penetration tester, and a seasoned software/security architect. He regularly teaches and speaks at technical colleges and conferences.

David is particularly interested in the interface between tech, psychology, and mathematics. He is a wholehearted teacher and mentor, and always looking to build bridges that help individuals and organizations grow.

Colin Murphy
Threat Intelligence

David Fuhr
Innovation & Cohorts

David Obando
Cloud & Cloud Security

Dror-John Röcher
Cyber & Strategy

Hauke Gierow
Communications & Cyber

Janis König
Deep Tech

Kalina Sperber
IT Security

Marc Nickert
Development

Nathalie Thomsen
Cohorts & Culture

Nils Brinker
Compliance & ISMS

Tobias Hellmann
IT Security & IR

int^3

intcube GmbH, 2024
Unconsulting cybersecurity. At scale.

hello@intcube.io
www.intcube.io

English

What our customers say

"The excellent staffing of key positions – such as the role of IT security officer – is essential for us.

With intcube, we had a partner who not only took over responsibility temporarily during a vacancy, but also significantly advanced our IT security.”

Ralf Oestereich, Board Member IT and Organization

SDK
Einfach für Ihr Leben da.

English

What our customers say

“We highly value our partnership with intcube. The team employs a data-driven approach that is strategic and fast, backed by their extensive industry knowledge, deep-tech-expertise and experience.

This expertise makes intcube an invaluable partner, significantly contributing to the informed and secure decision-making processes of clients.”

Dan Bender, Founding Partner

Code & Co.

English

What our customers say

“Especially for us in the banking industry, it is essential to enrich the vulnerability management process with daily updated data. intcube has been significantly supporting us in implementing a cyber threat intelligence process that allows us to precisely prioritize and document security measures.
We are now better prepared to respond more effectively to cyber threats with targeted information.”

Leon von Dassel, Coordinator IT Security

Berlin Hyp

English

What our customers say

„intcube advised us on the introduction of the BSI IT Baseline Protection standard.
The consulting was excellently tailored to the specifics of a university and truly helped us develop the right strategy for solving this challenge.“

Prof. Dr. Martin Mauve, Vice-Rector for Digitalization and Scientific Infrastructure

hhu Heinrich Heine Universität Düsseldorf

English

What our customers say

"In the world of IT security, it is essential to maintain an overview at all times and react to changes with agility. Efficient and transparent processes are essential for this.

Working with intcube has enabled us to implement processes that not only provide continuous clarity and prioritization, but also effectively optimize our IT security."

Jovi Trifkovic, Head of IT Platforms and Services

SDK
Einfach für Ihr Leben da.

English

What our customers say

"When it comes to detecting and defending against cyber attacks, the public administration has a great need but limited resources. intcube not only provides in-depth expertise in cyber security, but also extensive experience with the requirements of the federally organized administration, especially in the design of collaboration models.
This enabled the team to develop a concept for a collaborative approach to detecting and defending against attacks for the govdigital members, which creates synergies and thus addresses the acute need in the best possible way under the existing framework conditions."

Uwe Schwarz, Chief Information Security Officer & Head of Business Unit Cybersecurity

GOVDIGITAL

English

What our customers say

"We were looking for a security partner who could support us both strategically and operationally. intcube proved to be the ideal partner in this context, mastering all aspects of a successful cybersecurity strategy and at the same time implementing the missing components with an explicit “hands-on” mentality.
In doing so, intcube navigated the complexity of a heterogeneous organization with ease and positively surprised us in every respect.“

Andreas Török, Managing Director netgo production

netgo