ENGAGEMENT PACK

Cybersecurity due diligence for private equity

Six engagements, mapped to the points in a deal and the hold period where cyber decides value. Scope and deliverables are set out in full. Commercial terms are agreed against the mandate.

Michael J. Loginov

Independent cyber due diligence and transaction advisory

mike@loginov.me · +66 933 299 000 · michaelloginov.com · linkedin.com/in/mikeloginov

How I work

Every engagement is delivered by me. There is no team behind the proposal that you do not meet, and no junior analyst writing the report. That constrains how much work I take on, which is the point.

The output is written for the person making the investment decision, not for the security function. A finding that cannot be expressed as a cost, a timeline and a decision has not been finished.

I have run these estates rather than only reviewed them. Sixteen security leadership mandates across global, group, executive director and advisory remits, from greenfield builds at sovereign scale to industrial crisis recovery. In several of them the CISO reported to me. Remediation estimates come from having delivered the work, not from a benchmark table.

I have no product to sell, no managed service to upsell and no downstream remediation contract to protect. The recommendation is the deliverable.

THE SIX ENGAGEMENTS

ENGAGEMENT	DURATION	DEAL STAGE	PRIMARY OUTPUT
01 Red Flag Screen	7 to 14 working days	Pre-LOI	One-page screen. Proceed, price or walk
02 Confirmatory Diligence	3 to 4 weeks	Exclusivity	Investment committee paper with priced findings
03 First 100 Days	3 to 12 months	Post-close	Executed remediation plan and interim leadership
04 AI Governance Review	3 weeks	Any stage	Gap assessment against EU AI Act and ISO/IEC 42001
05 Fractional or Interim CISO	6 to 24 months	Hold period	An accountable security leader and a functioning team
06 Non-Executive Board Advisor	12 months, rolling	Any stage	Independent challenge on cyber and AI in the board pack

Engagements are sized to the mandate and the pace of the transaction. They can be run individually or in sequence across the deal lifecycle and the hold period. Delivered on site or remotely across Asia, Europe and the Middle East.

01 Red Flag Screen

A fast, outside-in read on a target before terms are set

DURATION	DEAL STAGE	ACCESS REQUIRED
7 to 14 working days	**Pre-LOI**	**Minimal**

WHAT I DO

- External attack surface and exposure analysis, conducted without contact with the target where confidentiality requires it.
- Breach and incident history research, including leaked credential exposure and dark web presence.
- Assessment of the target's regulatory position, including NIS2, DORA and sector obligations where they apply.
- Where management access is available, a single structured session with the senior technology or operations lead.
- Identification of anything that should stop the deal or change the terms before you commit to exclusivity.

WHAT YOU RECEIVE

- A one-page screen with a clear recommendation: proceed, proceed with conditions, or walk.
- Traffic light rating across eight domains, with the basis for each rating stated.
- An indicative remediation cost range, given as a band rather than a point estimate at this stage.
- A short list of the questions to press in confirmatory diligence, and where management is most likely to be optimistic.
- A verbal debrief with the deal team, usually within 24 hours of the written output.

WHAT THIS IS NOT

This is not confirmatory diligence and should not be relied on as such. A screen of this length buys you a view on whether the risk is worth investigating properly, and on whether the terms should reflect it. It does not buy you a defensible position for the investment committee.

02 Confirmatory Diligence

Findings quantified in terms an investment committee can price

DURATION	DEAL STAGE	ACCESS REQUIRED
3 to 4 weeks	**Exclusivity**	**Full**

WHAT I DO

- Management interviews across technology, operations, finance and, where relevant, plant engineering.
- Documentation and evidence review against the target's own operating model rather than a generic framework.
- Site inspection where operational technology, industrial control systems or physical estate are material.
- Assessment of the full estate: IT, OT, IoT, ICS and AI. Most under-priced risk sits outside the IT boundary.
- Costing of each material finding into a one-off figure, a permanent run-rate figure and a delivery timeline.
- Modelling of value at risk against the target's own revenue concentration and operational dependencies.

WHAT YOU RECEIVE

- An investment committee paper, written to be read by people who are not security specialists.
- A risk heat map plotting each finding by operational impact and assessed likelihood over the hold period.
- Cost to remediate and time to defensible, built line by line so that every figure can be walked and defended.
- A price adjustment argument where the evidence supports one, separating capital cost from permanent EBITDA effect.
- Recommended SPA positions, including where a specific indemnity is needed rather than a general warranty.
- Attendance at the investment committee to present and defend the findings, at no additional cost.

WHAT THIS IS NOT

This is not a penetration test, a compliance audit or a certification exercise. Where intrusive technical testing is warranted I will say so and can specify it, but it sits outside this engagement.

03 First 100 Days

Turning diligence findings into a de-risked asset

DURATION	DEAL STAGE	BASIS
3 to 12 months	**Post-close**	**Fractional or interim**

WHAT I DO

- Convert the diligence findings into a sequenced remediation plan built around the asset's operational constraints.
- Establish accountable security leadership, whether by recruiting it, standing in as interim CISO, or both.
- Post-merger integration of security and technology governance where the asset is a platform or bolt-on.
- Build the board and sponsor reporting line so that cyber risk is visible in the same cadence as financial performance.
- Where required, act as interim CISO or CAIO through the transition rather than advising from the outside.

WHAT YOU RECEIVE

- A prioritised remediation roadmap with owners, sequencing and the operational windows the work must fit into.
- A governance structure that survives the sponsor's reporting requirements and the eventual exit process.
- Quarterly progress reporting written for the sponsor, showing risk reduced rather than tasks completed.
- A capability that continues after I leave, including the specification and recruitment of the permanent hire.
- Evidence packaged as it is generated, so that exit diligence is a retrieval exercise rather than a reconstruction.

WHAT THIS IS NOT

This is not a staff augmentation arrangement and it is not an outsourced security function. The objective is a management team that no longer needs me.

04 AI Governance Review

AI risk assessed with the discipline investors expect of financial and legal diligence

DURATION	DEAL STAGE	FRAMEWORKS
3 weeks	**Any**	**EU AI Act, ISO 42001**

WHAT I DO

- Inventory of AI systems in use, in development and embedded in third party products, which is usually where the surprises are.
- Classification against EU AI Act risk tiers, with a clear position on which obligations apply and by when.
- Gap assessment against ISO/IEC 42001 and the NIST AI Risk Management Framework.
- Assessment of model provenance, data rights and the contractual position on training data, which carries real deal risk.
- A board or investment committee workshop to establish where accountability for AI risk actually sits.

WHAT YOU RECEIVE

- A gap assessment with obligations mapped to deadlines and to named owners.
- An implementation roadmap costed to the same standard as the cyber remediation plan.
- A written position on AI-related deal risk suitable for inclusion in the investment committee paper.
- Executive workshop materials and a governance framework the business can operate without external support.

WHAT THIS IS NOT

This is not a legal opinion on the EU AI Act and does not replace counsel. It establishes the factual and operational position that legal advice is then given against.

05 Fractional or Interim CISO

Accountable security leadership without a permanent hire

DURATION	COMMITMENT	BASIS
6 to 24 months	**2 to 4 days a month, or full time**	**Fractional or interim**

WHAT I DO

- Hold the CISO accountability formally, reporting to the board, the audit committee or the sponsor.
- Own the security strategy, budget and roadmap, and the decisions about what is not being done and why.
- Lead the existing function, or build one, including structure, hiring specification and supplier consolidation.
- Represent security externally: to clients in their own diligence, to insurers at renewal, and to regulators where DORA, NIS2 or sector rules apply.
- Lead the response if a material incident occurs on watch, including board and sponsor communications.
- Specify and recruit the permanent successor, then hand over against a documented plan.

WHAT YOU RECEIVE

- A named, accountable security leader at a fraction of the cost of a permanent executive hire.
- Board and audit committee reporting in the cadence the sponsor expects, written in business terms.
- A costed roadmap that survives challenge, and a team capable of delivering it.
- Client-facing and insurer-facing assurance, which frequently unblocks revenue that a security gap was holding up.
- Continuity of judgement across the hold period rather than a sequence of short consulting engagements.
- A documented handover to the permanent CISO, with the capability left standing.

WHAT THIS IS NOT

This is not a part-time consultant without authority. The role carries accountability and the decisions that go with it. Nor is it intended to be permanent: the measure of success is a business that no longer needs the arrangement.

06 Non-Executive Board Advisor

Independent challenge on cyber and AI risk at the top table

DURATION	COMMITMENT	BASIS
12 months, rolling	**Board cycle, plus call-off**	**Advisory or non-executive**

WHAT I DO

- Sit on the board or advisory board, or attend the audit and risk committee as the cyber and AI specialist.
- Challenge the executive's reporting: whether the risk position presented is the real one, and whether the assurance behind it holds.
- Advise the chair or the sponsor privately on where the reported position and the operational reality diverge.
- Support the sitting CISO rather than displace them, including acting as a sounding board between meetings.
- Provide an independent read on cyber and AI readiness ahead of a fundraise, refinancing or exit.
- Review incident and near-miss reporting for what it says about the control environment rather than the incident.

WHAT YOU RECEIVE

- Independent challenge on the cyber and AI content of the board pack, before it reaches the buyer or the regulator.
- A cyber voice at the top table that is not reporting to the executive it is assessing.
- Early warning where a control gap is likely to surface in exit diligence, while there is still time to fix it.
- Access between meetings for the chair, the sponsor or the CISO when a decision cannot wait for the next cycle.
- An annual written opinion on the maturity trend, suitable for the sponsor's own reporting.

WHAT THIS IS NOT

This is not executive management and it is not the CISO role. Independence is the value, so I will not hold both positions in the same business at the same time.

Confidentiality and how information is handled

Cyber diligence involves being told, in writing, exactly where a business is weakest. That information is commercially sensitive to the sponsor and existentially sensitive to the target. How it is handled is part of the engagement, not an afterthought.

BEFORE ANYTHING IS DISCUSSED

Mutual NDA	A mutual non-disclosure agreement (MNDA) is put in place before a target is named. Mutual rather than one-way, because the method, pricing approach and working papers are mine, and the target and deal thesis are yours. I will work to your paper or provide a short form MNDA if that is faster.
Conflicts check	Run before any target is discussed in detail. If I hold a current mandate that conflicts, I will say so and decline rather than manage around it. Where I have prior knowledge of a target from an earlier engagement, that is disclosed before we proceed.
Clean team	Where a transaction requires clean team arrangements, I can work inside them and will sign the associated protocols. Competitively sensitive material is handled accordingly.

DURING THE ENGAGEMENT

- Target material is held only for as long as the engagement requires it, in an encrypted store under my sole control.
- No target information is placed in third party AI tools, cloud analysis services or shared drives.
- Where the target is not aware of the transaction, the work is scoped so that nothing I do signals it. Outside-in analysis is used in place of contact.
- Findings are reported to the commissioning party only. I do not brief the target, its management or any other bidder unless you instruct it in writing.

AFTER THE ENGAGEMENT

- Working papers and target material are destroyed or returned on request at engagement close, subject to any retention the MNDA or your own policy requires.
- The deliverable is yours. It can be shared with your investment committee, lenders and advisers without further permission.
- Engagements are not referenced publicly. Nothing in my own materials names a target, a sponsor or a transaction without written consent.

A NOTE ON ABORTED DEALS

Deals fall over, sometimes because of what the diligence finds. Where an engagement is stopped mid-flight, you are billed for work delivered to that point and the findings are handed over in whatever state they have reached, rather than withheld pending completion.

Commercial basis

Terms are agreed against the mandate rather than published, because the same engagement carries different value on a €30m carve-out and a €900m platform. What follows is how the work is structured.

Basis	Fixed-scope assignment · Retained · Day rate · Fractional or interim · Advisory or non-executive
Engaged	Directly by the sponsor, or through advisory, risk and consulting firms as a named specialist under their contract and brand
Mobilisation	Typically within five working days for a screen, ten for confirmatory diligence. Fractional and non-executive arrangements start at the next board or reporting cycle
Coverage	Asia, Europe and the Middle East. On site as the mandate requires, remote where it does not
Confidentiality	Mutual NDA before a target is named. Standard sponsor NDAs accepted. Conflicts checked before any target is discussed
Capacity	Engagements are taken in limited number so that each is delivered personally. Confirmatory diligence in particular is capacity constrained during exclusivity periods
Combining engagements	A screen credits against confirmatory diligence on the same target. Diligence findings carry directly into First 100 Days without a re-scoping exercise

WHERE I AM NOT THE RIGHT FIT

I am probably not the right choice if you need a twenty-person team, an audit sign-off, or a commodity compliance assessment. Those are legitimate requirements and there are firms built to meet them. My work is concentrated on complex transactions where experienced judgement informs the investment decision, and where the person who did the fieldwork is the person who defends it in the room.

NEXT STEP

A 30 minute conversation about the deal, under MNDA if preferred, is usually enough to establish whether the risk is worth investigating and which engagement fits.

Michael J. Loginov

UK CISO of the Year 2020 · UK Cyber Security Hall of Fame · Author, *CISO: Defenders of the Cyber Realm*

mike@loginov.me · +66 933 299 000 · michaelloginov.com