

Deloitte.



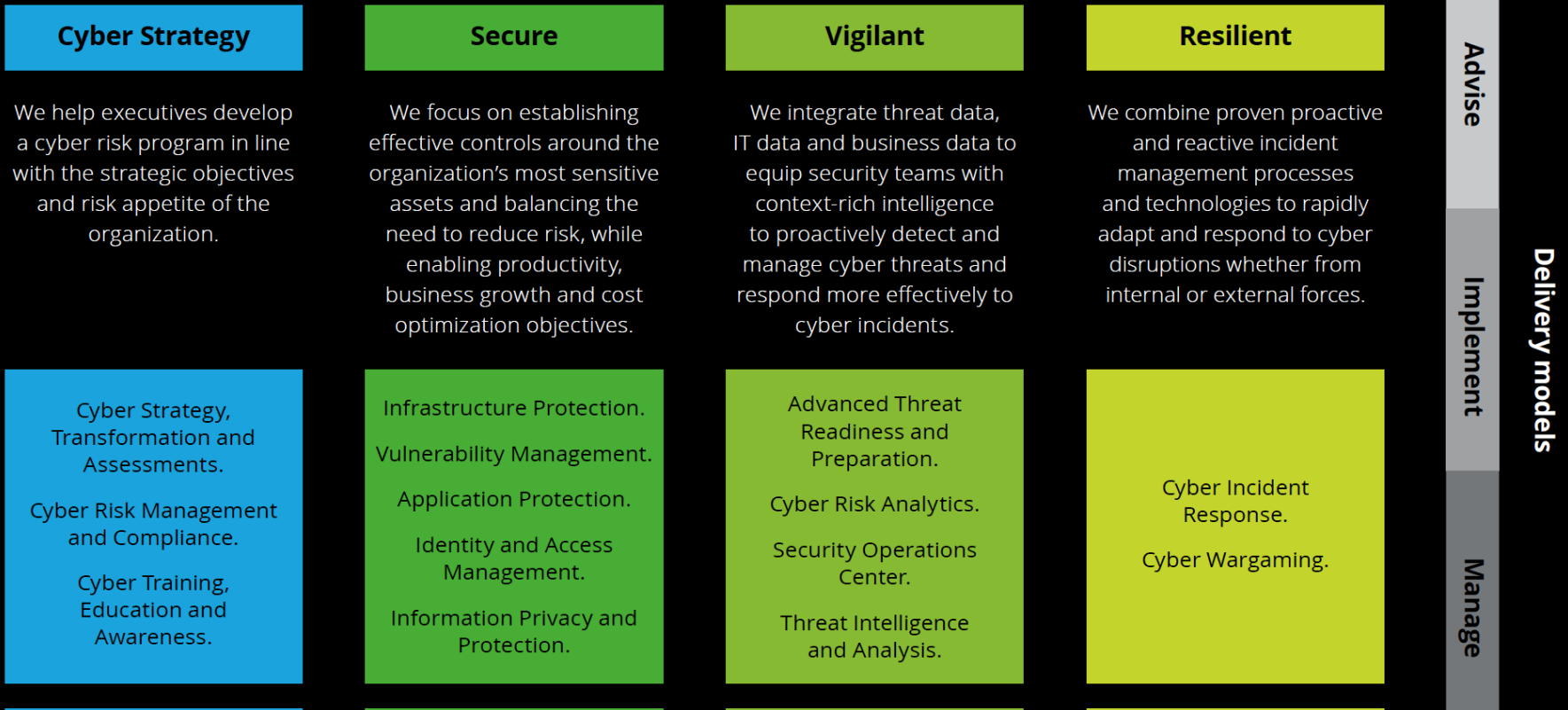
Cyber Risk & GDPR

Getting prepared for the new challenges

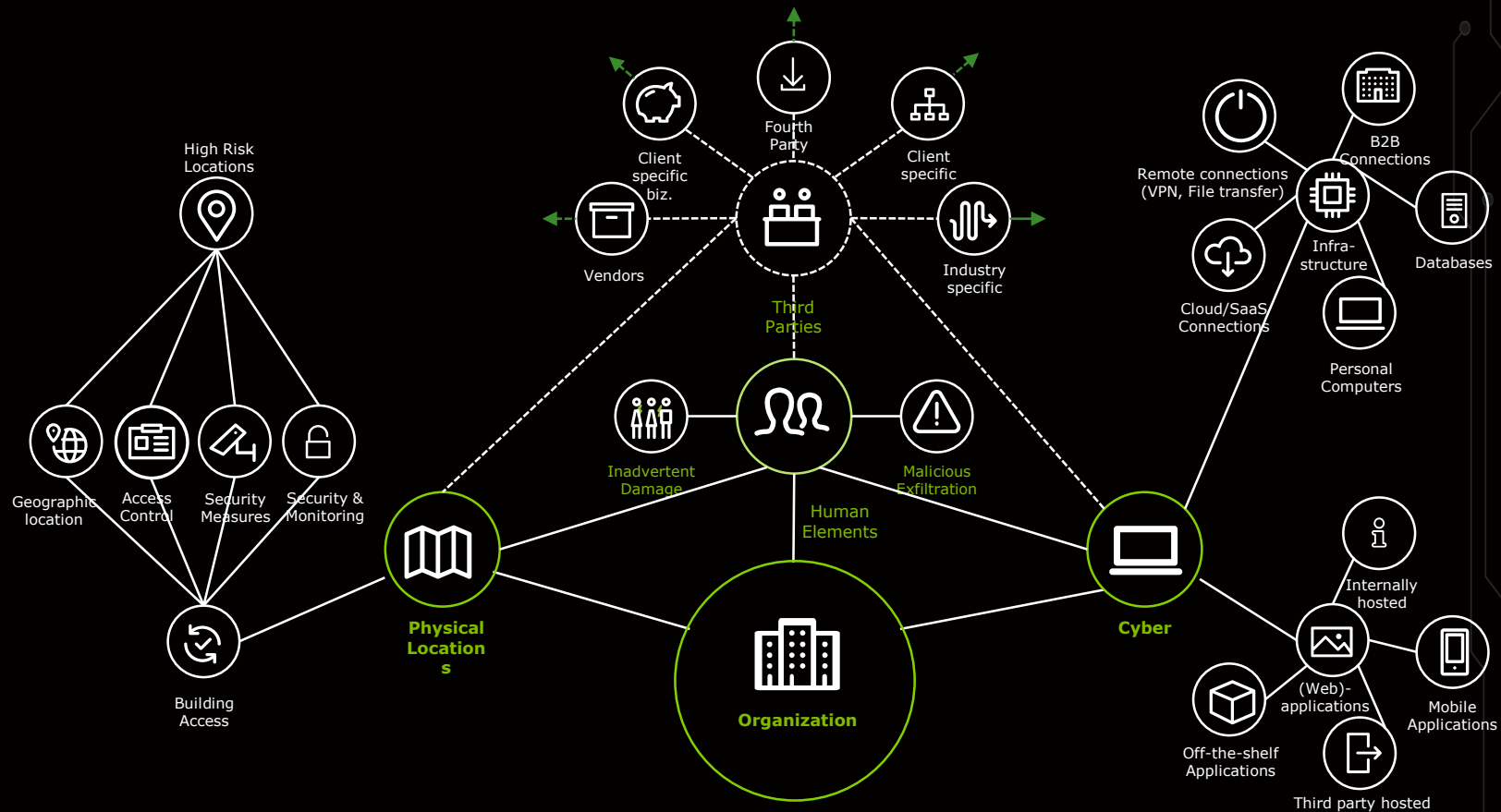
Adrian Ifrim, Deloitte Romania

Deloitte Cyber Risk

Delivery models



Attack surface – beyond the perimeter





Red Team

Realistic, simulated attack, following the profile of an actual threat actor to the organization. The red team will try and achieve a number of agreed objectives without raising any detection or response.



Purple Team

Combining the red and blue team efforts in an interactive setting: by performing an attack while the blue team is actively watching which elements are and are not detected. Afterwards, both blue and red team improve their approaches and retry.



Blue Team

Continuous monitoring of and response to indicators of attacks and compromises. To this end, the blue team establishes and improves on detection measures in the IT infrastructure and defines and implements specific "use cases" to monitor for.

How to

Measuring progress and achieving tangible improvement

Manageable scope

By predefining a very clear and limited scope, we ensure that we obtain a detailed view of effectiveness of specific measures, while keeping a keen eye on the larger context of actual attacks.

Measure improvement

Purple teaming is perfectly suited to measure effectiveness of newly implemented detection technology and to verify that actual progress is made during larger security transformations.

Iterative approach

By employing a step-by-step and iterative approach we allow for multiple phases of improvements, each time taking both attack and defense to the next level.

Realistic scenarios

By leveraging our world-class knowledge of the current threat landscape for your industry and organization, we ensure that all simulations are in line with your actual risk profile.

Multi-disciplinary

Our approach includes people, processes and technology and we can supply experts on both the offensive and defensive sides, empowering your own staff where they need it most.



Lab environment

We perform attacks on a virtual environment, similar to your own. We show you how an attack works and what defenses can do to stop and detect them.

Hybrid lab

We setup a lab environment identical to a part of your infrastructure. This way, the purple team can work without any risk of impacting normal operations.



How we execute

Not every client has the same goals and needs from a purple teaming engagement. Just as not every client will have the option to perform multiple iterations of an attack in its actual environment. We can execute engagements in a variety of environments, from fully virtual to your actual infrastructure.

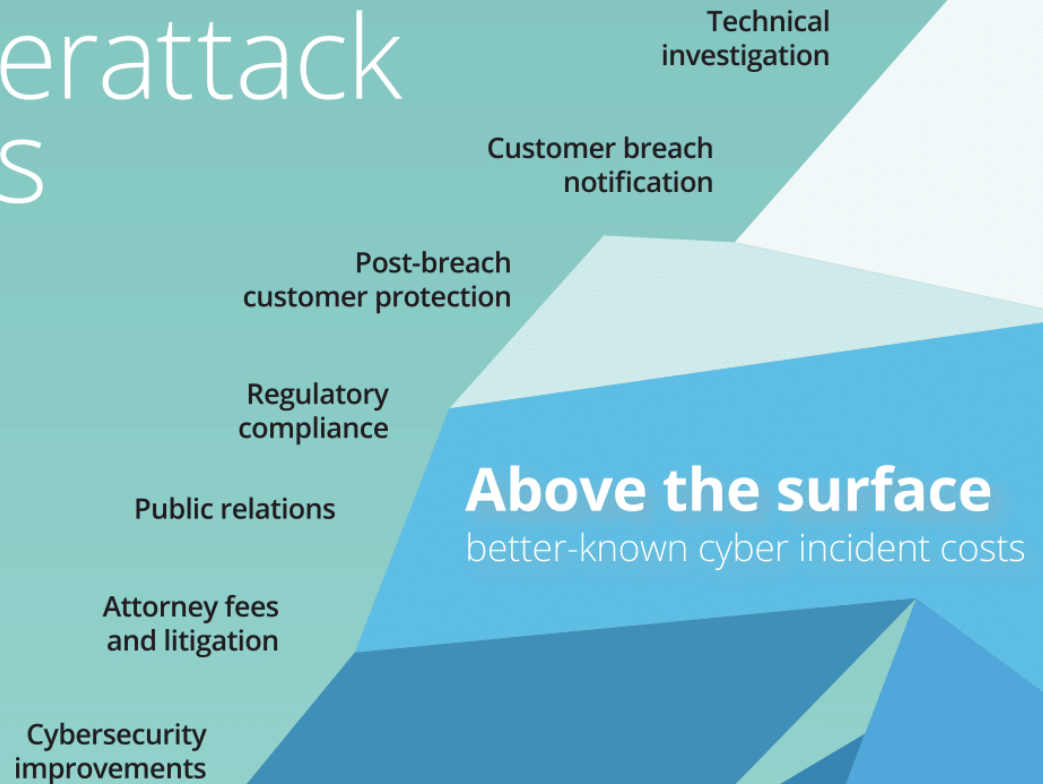
Your infrastructure

The most realistic option: we perform attacks and monitor defenses in your own infrastructure. We setup safeguards to prevent impact on business.



Fourteen cyberattack impact factors

A wide range of direct and/or intangible costs contribute to the overall impact of a major cyber incident.



Beneath the surface

hidden or less visible costs

Insurance premium
increases



Increased cost
to raise debt

Impact of operational
disruption or destruction



Lost value of customer
relationships

Value of lost
contract revenue



Devaluation of
trade name

Loss of intellectual
property

CONTACTS

Your domain experts access



Partner Risk Advisory, Romania

Andrei Ionescu

Partner leading the Risk Services in the Romania & Moldova practice. Andrei has more than 18 years of experience in Risk Management, Cyber Risk, Internal Audit, Fraud Management, Information Systems Audit, Business Continuity / Disaster Recovery and Revenue Assurance.

Andrei is a certified expert in fighting against corruption, CISA (Certified Information Systems Auditor), CRISC (Certified in Risk and Information Systems Control), CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager), Certified Project Manager.

Email: aionescu@deloitte.com



Manager Risk Advisory | Cyber Risk Services, Romania

Adrian Ifrim

Adrian is a Manager in Risk Advisory with more than ten years of experience in the IT security field working for financial and telecom institutions.

Adrian held technical security related positions within ING Bank N.V., Amsterdam - Bucharest Branch, UniCredit Bank România and Vodafone România. He currently holds the Offensive Security Certified Expert (OSCE), Offensive Security Certified Professional (OSCP) certifications and Systems Security Certified Practitioner (SSCP).

Email: aifrim@deloitte.com



Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee (“DTTL”), its network of member firms, and their related entities. DTTL and each of its member firms are legally separate and independent entities. DTTL (also referred to as “Deloitte Global”) does not provide services to clients. Please see www.deloitte.com/about to learn more about our global network of member firms.

Deloitte provides audit, consulting, financial advisory, risk advisory, tax and related services to public and private clients spanning multiple industries. Deloitte serves four out of five Fortune Global 500® companies through a globally connected network of member firms in more than 150 countries and territories bringing world-class capabilities, insights, and high-quality service to address clients’ most complex business challenges. To learn more about how Deloitte’s approximately 245,000 professionals make an impact that matters, please connect with us on Facebook, LinkedIn, or Twitter.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the “Deloitte Network”) is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte Network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.