Deloitte.

Cyber Risk & GDPR

Getting prepared for the new challenges

Adrian Ifrim, Deloitte Romania

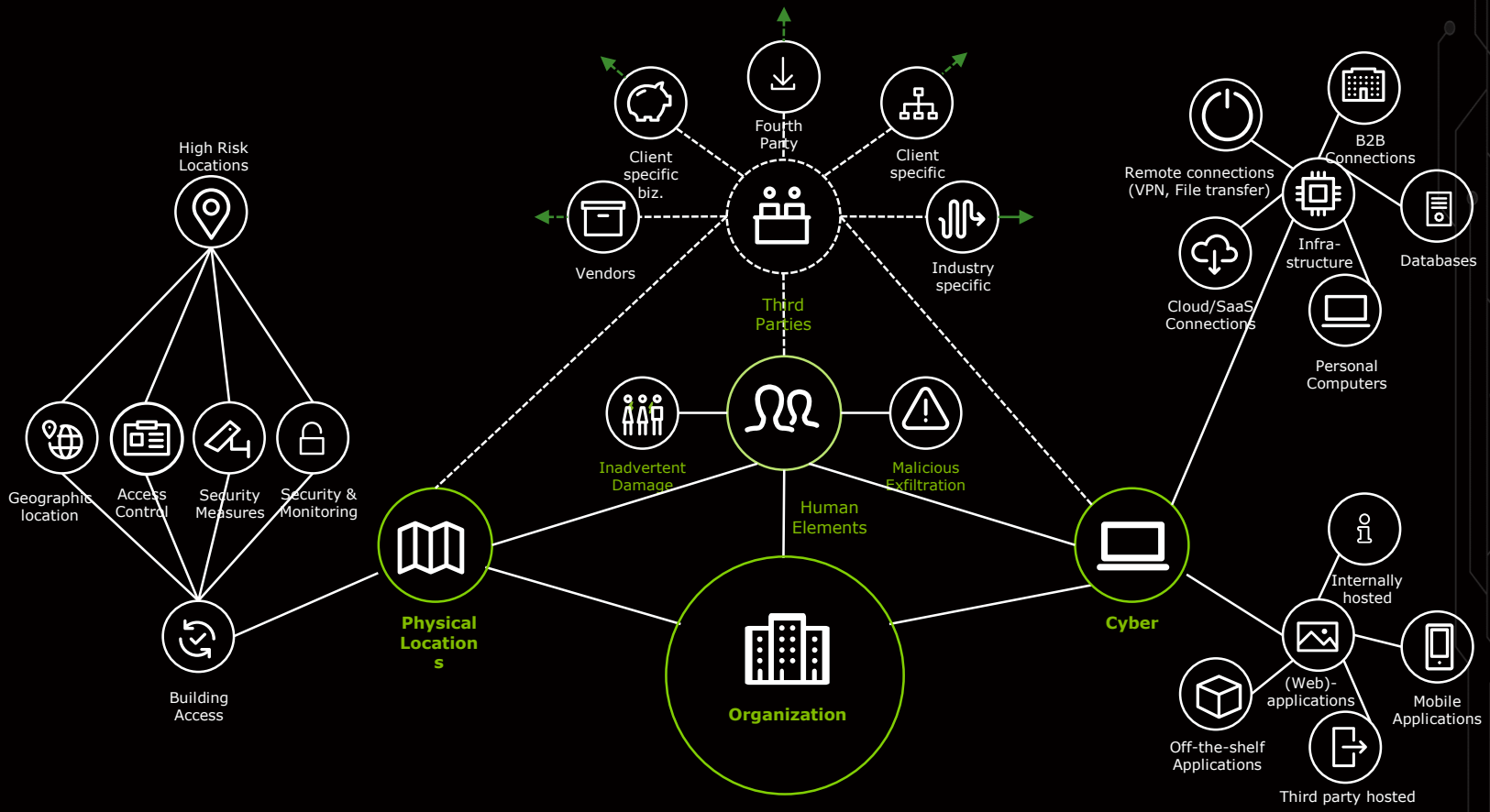
Deloitte Cyber Risk

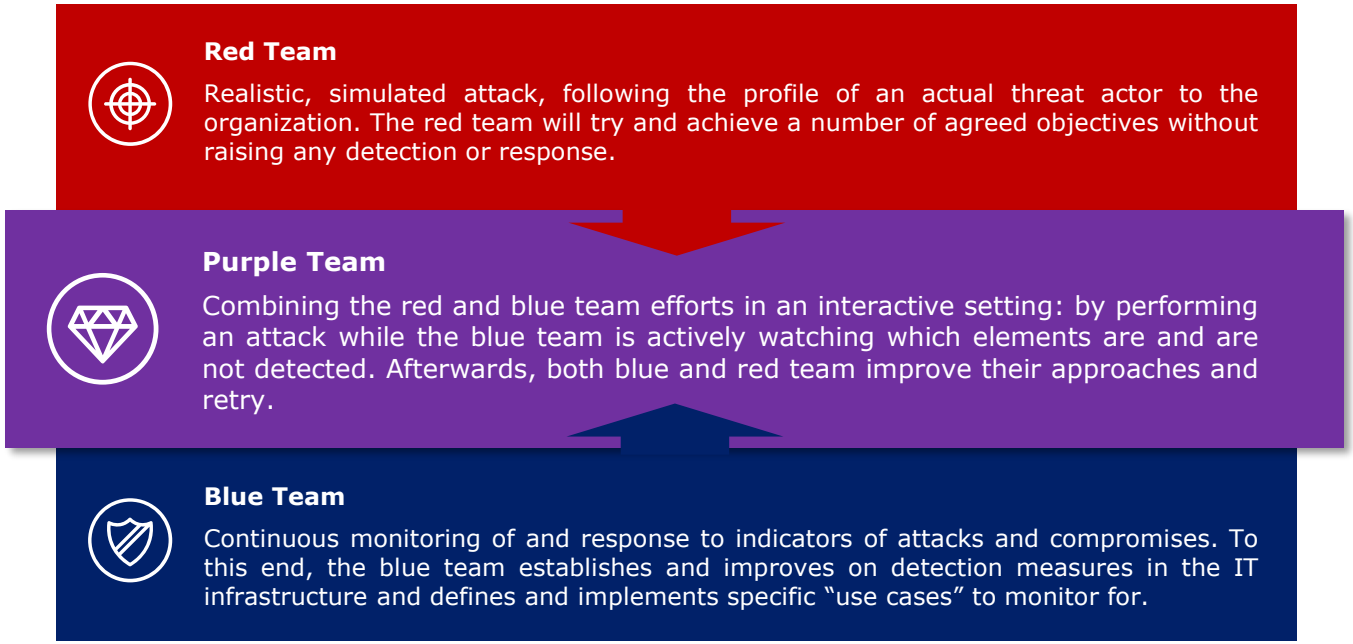
Delivery models

Cyber Strategy	Secure	Vigilant	Resilient
We help executives develop a cyber risk program in line with the strategic objectives and risk appetite of the organization.	We focus on establishing effective controls around the organization's most sensitive assets and balancing the need to reduce risk, while enabling productivity, business growth and cost optimization objectives.	We integrate threat data, IT data and business data to equip security teams with context-rich intelligence to proactively detect and manage cyber threats and respond more effectively to cyber incidents.	We combine proven proactive and reactive incident management processes and technologies to rapidly adapt and respond to cyber disruptions whether from internal or external forces.
Cyber Strategy, Transformation and Assessments. Cyber Risk Management and Compliance. Cyber Training, Education and Awareness.	Infrastructure Protection. Vulnerability Management. Application Protection. Identity and Access Management. Information Privacy and Protection.	Advanced Threat Readiness and Preparation. Cyber Risk Analytics. Security Operations Center. Threat Intelligence and Analysis.	Cyber Incident Response. Cyber Wargaming.

Advise
Implement
Manage
Delivery models

Attack surface – beyond the perimeter





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.

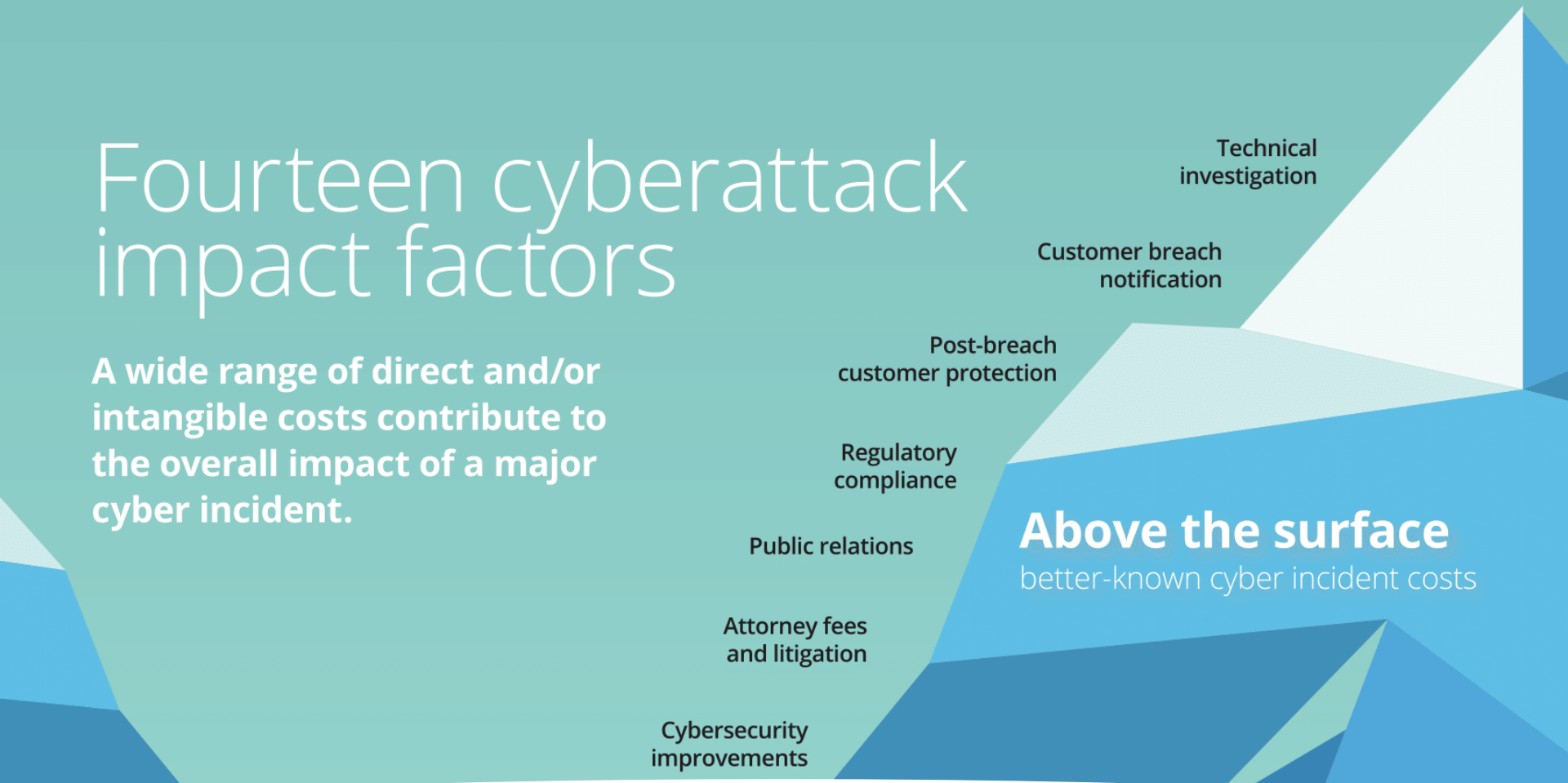
Hybrid lab
We setup a lab environment identical to a part of your infrastructure. This way, the purple team can work without any risk of impacting normal operations.

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.

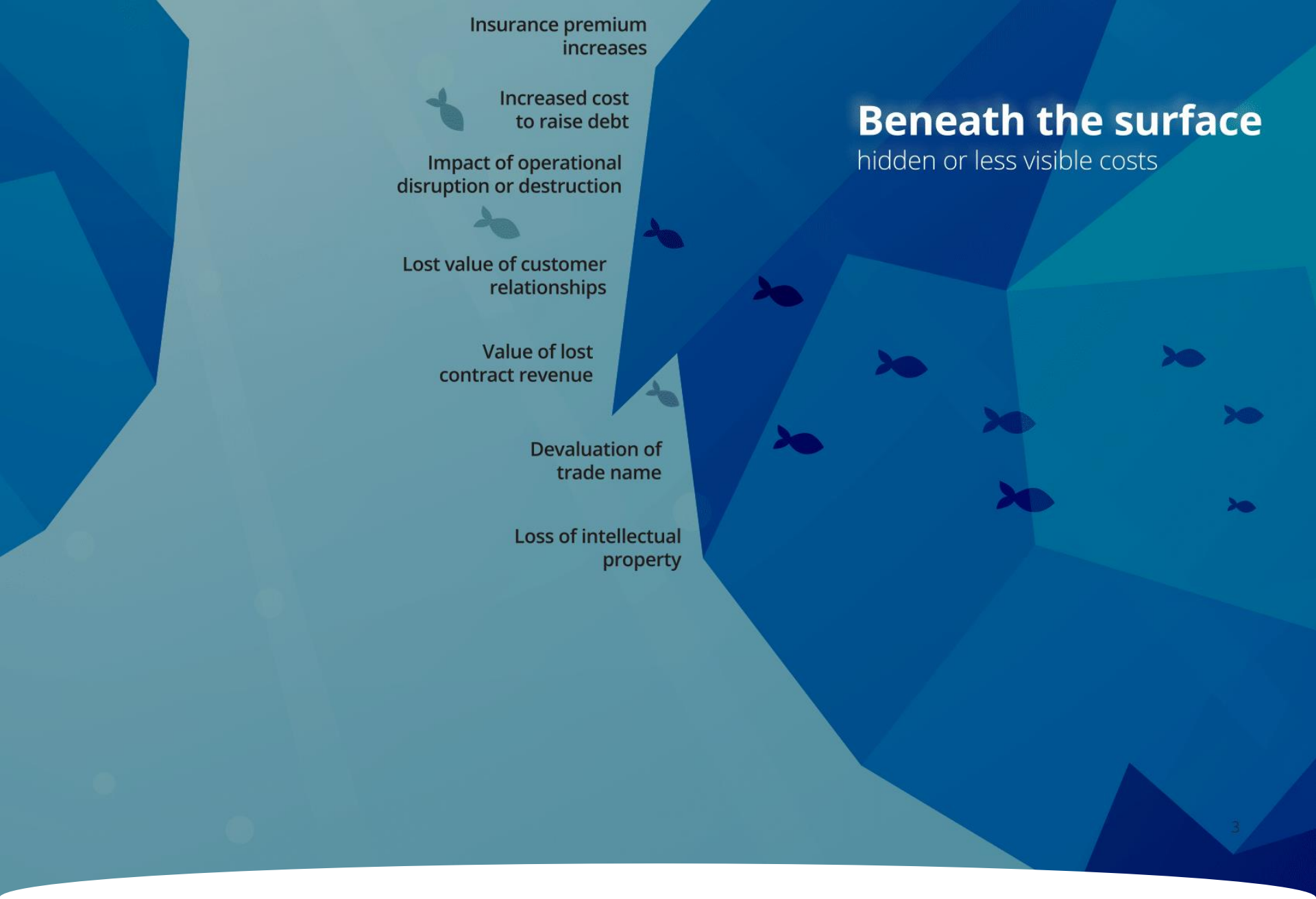
Fourteen cyberattack impact factors

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



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.