

# Proactive DFIR in the CISO toolkit

Dimitris Georgiou, CSO-Partner



# Who we are

## AlphaBit

- was founded in 2008, providing a complete set of Information Technology and Cybersecurity Services
- has a team of certified and highly-qualified engineers, tackling complex IT and cybersecurity projects
- has doubled its turnover, sales and workforce over the last 2 years
- cooperates with major IT and Cybersecurity manufacturers: Acronis, Belkasoft, Comodo, Dell, Fortinet, Grandstream, HPE, Microsoft, KnowB4, Veritas, and others



# Alpha**bit** 360

Protect your business

- IT Management
- Risk Management
- Security Management
- Digital Forensics

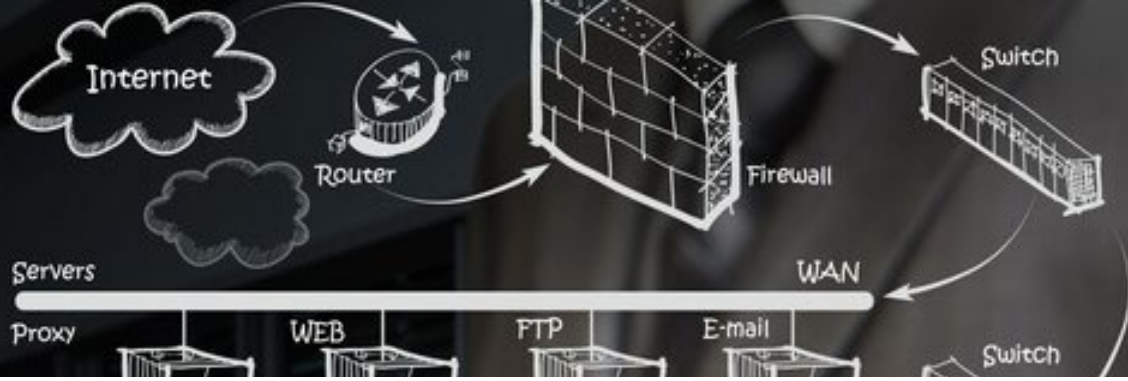


# Digital Forensics & Incident Response

what we do

## Alphabit

- responds to incident handling requests, contains, remediates and provides root cause analysis services and lessons learned consulting
- offers digital forensics services (data recovery, acquisition and investigation) for corporate clients, law firms and government agencies since 2010
- holds relevant certifications and expertise on a multitude of forensic technologies and techniques
- has created the “Alphabit Forensics Laboratory” using an extensive toolkit, and forensically sound processes
- provides Expert Technical Reports (to be also used as evidence in court proceedings), Expert Testimony and Consulting for law firms



If you feel uncertain, risk assess!

If you feel certain, learn more!

If you feel strong, pen test!

If you feel safe, don't.



Dimitris Georgiou  
CSO-Partner



**US**

Good guys, the blue  
teamers



**THEM**

Bad guys, the  
attackers, the  
threat actors,

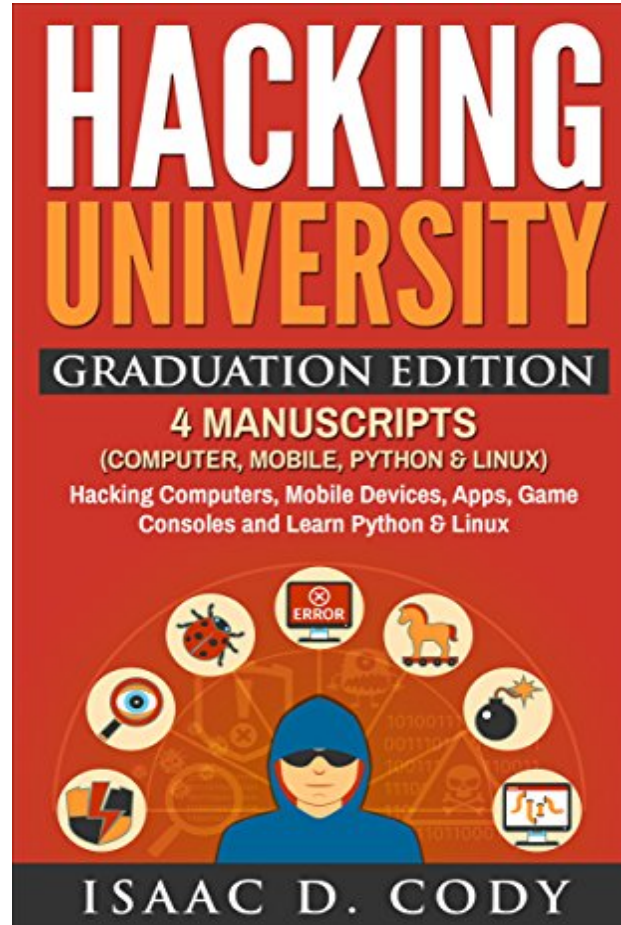


The eternal battle

# Threat actor agenda

What do they do?

- Stay anonymous
- Bot-herd
- Produce malware
- Propagate spam/phishing
- Manipulate people
- Exploit data
- Steal infrastructure
- Deny service





What do Infosec Professionals Do?

- Budget
- Security Operations
- Business Enablement
- Project Delivery Lifecycle
- Identity Management
- Security Architecture
- Governance
- Compliance and Audits
- Team development
- Selling Infosec (Internal)
- Risk Management
- Training and Exercises

Incident Response

Investigations and Forensics



## Chief Information Security Officer

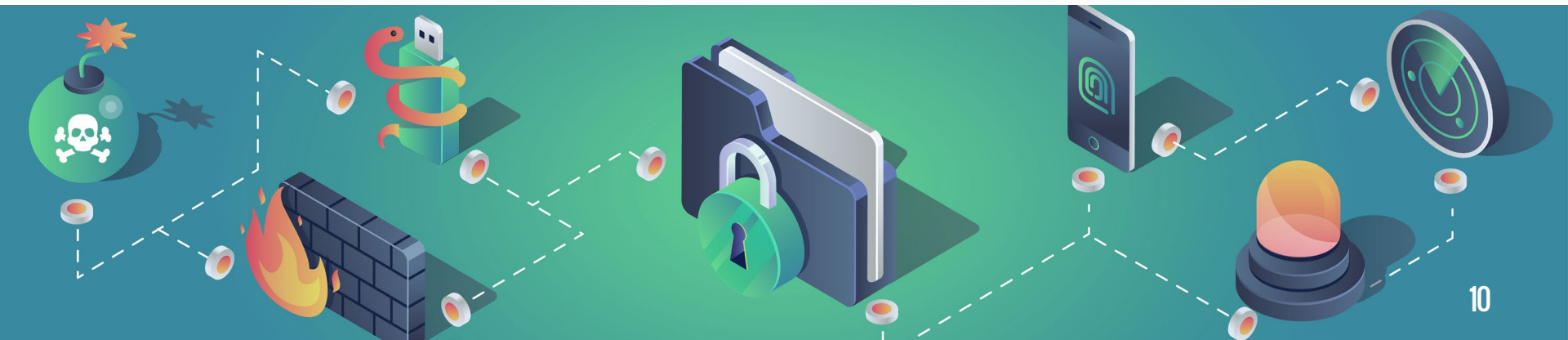


**But even if the CISO performs 99% of his tasks perfectly, there is still the possibility that a small mistake could cause a big problem.**



Cyberattacks are on the rise, indicators reflect a fear of further attacks. What next?

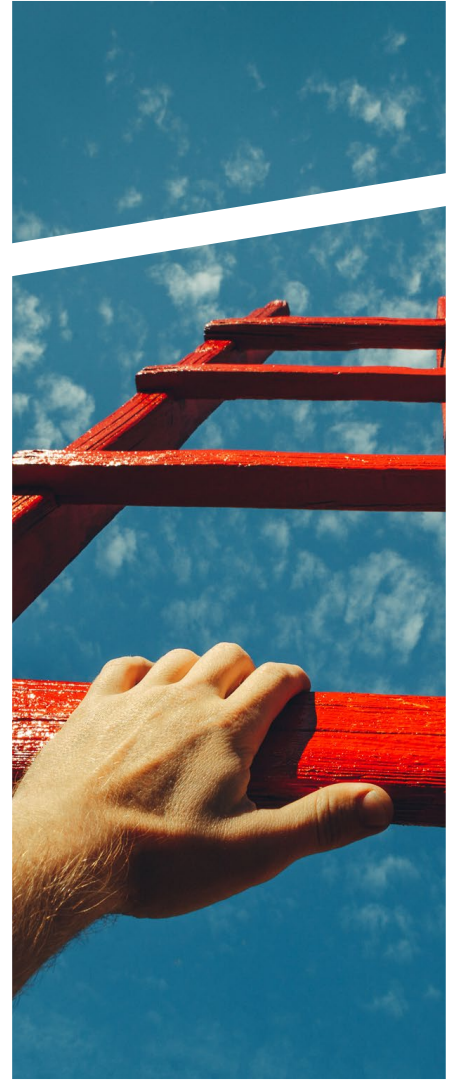
Alphabit





# And what about the big challenges brewing for the future?

- ✓ New legal framework for cybersecurity and data privacy
- ✓ New technologies and solutions
- ✓ Talent acquisition
- ✓ Greater workload



# Why proactive DFIR?

- ✓ Minimize the impact of cyber attacks for your business
- ✓ Prove to insurance companies that you have adopted a proactive approach to cyber security, thus lowering your risk profile and reducing premiums
- ✓ Part of an effective cyber security strategy
- ✓ Ready to react fast




# Why DFIR with a partner?

- ✓ Complement internal ability on incident response
- ✓ Assist with mundane tasks
- ✓ Provide proven expertise on incident investigations
- ✓ Mediate between IT/Infosec and Legal/Compliance teams
- ✓ Act as an Independent respondent and forensic investigator









**Our team of experts is here to provide cutting-edge consulting and superior know-how to successfully meet your demands on DFIR and help you protect your business well before the actual incident occurs.**





# Thank you!

