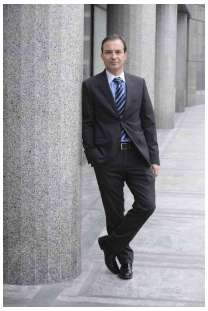
Mr Nikos Mourtzinos,
Security Product Specialist, Cisco Systems Hellas



Short Curriculum Vitae (C.V.)

Nikos is the Cisco Security and Data Center Product Sales Specialist for Cisco Greece, Cyprus and Malta. He has been with Cisco since August 2010. He is responsible for the Cisco Security Products and solutions. Before joining Cisco, Nikos was the Line of Business Manager of HP Network Solution Group. He worked for HP for ten years and his main focus was the overall management of the "Network Solution Group" of HP Hellas. Before joining Hewlett-Packard, Nikos was a network consultant and gained international experience by working for IBM Global Services Hellas for five years.
He studied Electrical Engineering at Aristotle university of Thessaloniki, Faculty of Engineering and M.Sc. in Data Telecommunications and Networks at University of Salford, Manchester, UK. He is also a Cisco Certified Internetwork Expert CCIE #9763.

"Failure of Legacy Security Architectures and the Importance of the new Cisco Threat focused Next-Generation Security"

Cyber attacks are becoming more sophisticated. Your business needs an equally sophisticated way of staying secure.
Legacy Security Architectures are not effective anymore in Maritime - Oil & Gas environments.
Moreover throughout industry—in oil fields, power plants and more—Digital Transformation and the Internet of Things (IoT) is boosting production. It's speeding delivery of products/services.
And it's helping companies like yours compete.
But while IoT is making you more efficient, the increased connectivity also makes your industrial control systems (ICSs) more vulnerable to cyberthreats.
We will present next-generation technologies for defending your critical infrastructure and offer threat prevention for both known and zero-day attacks.

Block more threats and quickly mitigate those that do breach your defenses with the industry's first threat-focused Security Architecture.

Gain deeper visibility on users, servers, applications (including ICS protocols/applications)
Reduce complexity and cost by unifying security layers and automating tasks
Respond with agility to attacks (both known and zero-day attacks) with automation and actionable indications of compromise (IoCs)
Greatly decrease the time from detection to cleanup with retrospective security