Mr Nikos Mourtzinos

Short Curriculum Vitae (C.V.)

Nikos Mourtzinos is the Cisco Security Product Sales Specialist for Cisco Greece, Cyprus, Malta, Israel and Portugal. 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-Greece, 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.

HOW TO PROTECT AGAINST THE EVOLVING CYBER THREATS

The network security threat landscape is ever evolving, but always at the cutting edge are custom-written, stealthy threats that evade traditional security perimeter defenses. The Cisco® Cyber Threat Defense Solution provides greater visibility into these threats by identifying suspicious network traffic patterns within the network interior.

The three main functional components of the Cisco Cyber Threat Defense Solution:

● Generating network-wide security telemetry - NetFlow export from Cisco network devices

● Aggregating, normalizing, and analyzing NetFlow telemetry data to detect threats and suspicious behavior

● Providing contextual information to determine the intent and severity of the threat - User identity, endpoint device profiling, and posture information from the Cisco Identity Services Engine

The Cisco Cyber Threat Defense Solution presents a unified view of the traffic pattern analysis via NetFlow and relevant contextual information regarding that traffic, such as user identity, posture, device type, user policy, application information, and firewall context. This information is presented in a single pane of glass

With this information, the analyst can decipher the correct next steps to take concerning the threat in a timely, efficient, and cost-effective manner for advanced cyber threats such as:

● Network reconnaissance

● Network interior malware proliferation

● Command and control

● Data exfiltration

Through the Intrusion Prevention System (IPS) offerings, Cisco provides customers with unrivaled industrial control protection.. Cisco® IPS technology also inspects protocols to protect SCADA networks. Cisco IPS Sensors deliver high-performance intelligent detection with precision response, extending the IPS capabilities from the network edge to the data center for both IPv4 and IPv6 networks.

The following are examples of protocols and threats currently covered by the Cisco industrial control protection offering:

- Systems: SCADA, DCS, PLC, SIS, RTU

- Threats and protections

- Signatures are also provided to control legal activities to manage access or change