1. Will MACSec be able to prevent ARP cache poisoning attack?   
     
   NO, DHCP Snooping and Dynamic ARP Inspection (DAI) combination are effective mitigation techniques.

DAI intercepts all ARP requests & responses, verifies their authenticity before updating the switch’s local ARP cache or forwarding the packets to the intended destinations.

Intercepts each ARP packet and compares its MAC Address and IP Address info against the MAC-IP Bindings contained in a trusted binding table. (Table is dynamically populated by DHCP when feature enabled)

DAI can be configured to drop ARP packets with invalid IP Addresses  
DAI Implements a configurable rate-limit function that controls the # of incoming ARP packets

DHCP Snooping is a prereq to configure Dynamic ARP Inspection. Features are capable of intercepting DHCP messages crossing a switch and blocking bogus DHCP offers.

Uses trusted ports (DHCP Servers) and Untrusted Ports (Clients)

Builds and maintains a MAC-to-IP binding table that is used to validate DHCP Packets received from untrusted ports.

Discards all untrusted DHCP packets that are not consistent with the information in the binding table.

1. Will MACSec be able to prevent CAM Table overflow attack?

No it cannot. Mitigation techniques include PORT SECURITY on the switch. Allows MAC addresses to be specified on a particular switch port, or specify the maximum number of addresses a switch port can learn.