Case Study :

Q) Why EMET is removed in windows 10 and Windows Defender Exploit guard is added?

Q) What additional. Security windows Defender EG have?

EMET → Enhanced Mitigation Experience Toolkit

It is a freeware security toolkit for microsoft windows developed by Microsoft. It provides a unified interface to enable and fine-tune windows security features. It can be used as an extra layer of defensive against malware. attacks, after the firewall and before antivirus software

EMET has limited set of mitigation and it dosent have network protection. It has no Controlled folder access. Mainly it has no userfriendly UI such as Microsoft intune for deploying and managing Configurations and no Configuration manager. It dosnt have an audit mode

Mitegation available in WDEG but not in EMET.

- → Block low integrity images
- → Code integrity guard
- → Disable win32 system calls
- → Do not allow child process
- → Import address filtering
- → validate handle usage
- → Validate heap integrity
- → validate image dependency integrity

also → New attack surface reduction rules added
→ Has a user friendly UI
→ Controlled folder access that can block disk sectors.
→ Network protection but requires WDAV.