Assignment-2

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 defense against malware attacks, after the firewall and before antivirus software. It has limited set of mitigations and it doesn't have network protection. It has no controlled folder access. Mainly it has no user friendly User Interfaces such as Microsoft intune for developing & managing configurations and no configuration manager. It doesn't have an auditmode.

Mitigations available in WDEG but not in EMET

→ Block low integrity images
→ Code integrity guard
→ Disable extension points
→ Disable win32 system calls
→ Donot allow child process
→ Import addressing filtering (IAF)
→ Validate handle ussage
→ Validate heap integrity
→ Validate image dependency integrity
→ New attack surface reduction rules added
→ Has a user friendly User Interface
→ Controlled folder access that can block disk sectors
→ Network protection but requires WDAV.