Insert

Assignment - 2

EMET - Enhanced Mitigation Experience Toolkit

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

→ EMET has limited set of mitigation and it doesn't have network protection. It has no controlled folder access. Mainly it has no user friendly ⊗ such as Microsoft intune for deploying & managing configurations and no configuration manages. It doesn't have an audit mode.

* Mitigation available in WDEG int not in EMET
  - → B have low integrity images
  - → code integrity guard
  - → Disable extension points
  - → Disable win 32k system calls
  - → Do not allow child process.
  - → Import addressing filtering (IAF)
  - → Validate handle usage
  - → Validate heap integrity

→ Validate image dependency integrity

also
→ Now Attack surface reduction rules added.
→ Has a user friendly UI
→ Controlled folder access that can "work disk security.
→ Network protection dnt requires WDAV..