SECURE CODING

Q)Why EMET is removed in windows 10 and Windows Defender EG is having?

Sol) EMET, a security solution that provides protections against general hacking attack techniques, is getting **deprecated** as a standalone Windows client solution, that means that it won't get developed and no security updates will arrive for it in the near future. Organizations with older applications typically might use EMET to ward off common exploit techniques. Microsoft announced that EMET's protections are getting moved into the "Windows Defender Exploit Guard" feature of the Windows 10 "fall creators update. Microsoft announced that EMET efforts are bringing **parity between Windows 10 mitigation support and all of the mitigation features provided by EMET**. The statement seems to be a response to **a critique by the security organization CERT** that Windows 10 does not provide the additional protections that EMET does. CERT specifically pointed to Control Flow Guard (CFG) protections lacking in Windows 10, which protect against application memory corruption vulnerabilities.

Q) What additional security Windows Defender EG is having?

Sol) Microsoft Windows Defender Exploit Guard (EG) is an anti-malware software that provides intrusion protection for users with the Windows 10 operating system.

1) Windows Defender Smart Screen : The windows defender smart screen can block at first sight. It helps protect employees if they try to visit sites previously reported as containing phishing or malware, and to stop them from downloading potentially malicious files. It can

also help protect against fake advertisements, scam sites, and drive-by attacks.

2) Windows Defender Application Guard : Application Guard gives you protection against advanced, targeted threats launched against Microsoft Edge using Microsoft's Hyper-V virtualization technology. The functionality works with whitelisting: Users can designate trusted sites to browse freely. If a site is not trusted, Application Guard will open it in a container, completely blocking access to memory, local storage, other installed applications, corporate network endpoints, or any other resources of interest to the attacker.

3) User Account Control : User Account Control (UAC) protects users by preventing malware from damaging a machine, and helps organizations deploy a better-managed desktop. When this feature is enabled, apps and tasks always run in the security context of a non-administrator account, unless an administrator specifically authorizes administrator-level access to the system.

4) Windows Defender Device Guard : Defender Device Guard involves driver and application whitelisting. The feature changes from a mode where apps are trusted unless blocked by an antivirus solution, to a mode where the OS trusts only apps authorized by an enterprise. It operates on two components: The first, kernel mode code integrity (KMCI) protects kernel mode processes and drivers from zero-day attacks and other vulnerabilities by using HVCI

5) Windows Defender Exploit Guard : Defender Exploit guard includes exploit protection, attack surface reduction rules, network protection, and controlled folder access. It also provides legacy app protection including arbitrary code guard, blocking low-integrity images, blocking untrusted fonts, and exporting address filtering. This helps you audit, configure, and manage Windows systems and application exploit mitigations. "It also delivers a new class of capabilities for intrusion prevention.

6) **Microsoft Bitlocker** : Bitlocker is a full-drive encryption solution provided natively within Windows 10 Professional and Enterprise. It helps mitigate unauthorized data access by enhancing file and system protections, and renders data inaccessible if the computers are decommissioned or recycled.

7) **Windows Defender Credential Guard** : Defender Credential Guard uses virtualization-based security to isolate secrets, so that only privileged system software can access them--protecting from credential theft attacks. Enabling this feature offers hardware security and better protection against advanced persistent threats.