Credential Access Protection, Mitigation M1043 - Enterprise

Archived: 2026-04-05 18:43:54 UTC

Credential Access Protection focuses on implementing measures to prevent adversaries from obtaining credentials, such as passwords, hashes, tokens, or keys, that could be used for unauthorized access. This involves restricting access to credential storage mechanisms, hardening configurations to block credential dumping methods, and using monitoring tools to detect suspicious credential-related activity. This mitigation can be implemented through the following measures:

Restrict Access to Credential Storage:

- Use Case: Prevent adversaries from accessing the SAM (Security Account Manager) database on Windows systems.
- Implementation: Enforce least privilege principles and restrict administrative access to credential stores such as `C:\Windows\System32\config\SAM`.

Use Credential Guard:

- Use Case: Isolate LSASS (Local Security Authority Subsystem Service) memory to prevent credential dumping.
- Implementation: Enable Windows Defender Credential Guard on enterprise endpoints to isolate secrets and protect them from unauthorized access.

Monitor for Credential Dumping Tools:

- Use Case: Detect and block known tools like Mimikatz or Windows Credential Editor.
- Implementation: Flag suspicious process behavior related to credential dumping.

Disable Cached Credentials:

- Use Case: Prevent adversaries from exploiting cached credentials on endpoints.
- Implementation: Configure group policy to reduce or eliminate the use of cached credentials (e.g., set Interactive logon: Number of previous logons to cache to 0).

Enable Secure Boot and Memory Protections:

- Use Case: Prevent memory-based attacks used to extract credentials.
- Implementation: Configure Secure Boot and enforce hardware-based security features like DEP (Data Execution Prevention) and ASLR (Address Space Layout Randomization).

Source: https://attack.mitre.org/mitigations/M1043