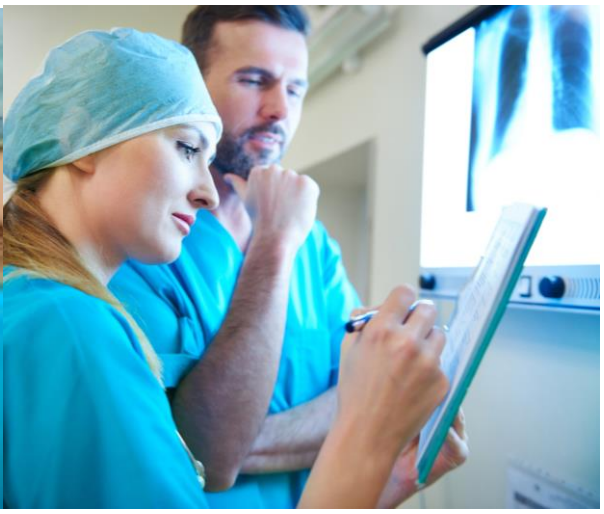
Healthcare Provider

Credential Visibility Sheds Light on Dangerous Software Flaw



If attackers are able to gain a foothold inside a network, they can harvest and exploit unseen credentials to move laterally toward critical business assets. Visibility into the credentials and connections inside a network is critical in minimizing vulnerability and exposure to cyberattacks.

A healthcare provider called Illusive in to investigate their environment and discover credential vulnerabilities. Using Attack Surface Manager, Illusive discovered that a recently installed security product in their network had a major bug, resulting in clear-text domain admin passwords being left on thousands of machines. If attackers were to land on any of these machines, these credentials could be exploited to accelerate access to critical systems and establish domain persistence—opening the door to severe damage.

The customer informed the security product vendor, who issued a patch to fix the issue. The customer acknowledged that despite having PAM and many other technologies in the SOC, they could not have discovered this critical condition without Illusive.

For more information, visit us at www.illusivenetworks.com
or email us at info@illusivenetworks.com