AuditScripts

Auditing Anti-Malware

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Anti-Malware

AuditScripts 5 Crucial Questions (v2.2)

Purpose:

Organizations audit their information security stance to protect the confidentiality, integrity, and availability of their information systems. Auditing and assessment allow an organization to validate their compliance with the standards they have set for themselves and to measure the levels of risk they are currently accepting.

AuditScripts has created the "5 Crucial Questions" series of audit checklists to provide auditors with a list of the five most important questions to ask when auditing a specific scope. Heavily influenced by the 20 Critical Security Controls project, these questions should serve as the starting point for any assessment.

5 Crucial Questions to Ask:

When performing an audit of an organization's anti-malware systems and their ability to defend themselves against malicious code, auditors should consider at a minimum asking the following questions:

1. What percentage of the organization's computer systems have up-to-date, centrally managed anti-malware software actively running?
2. What percentage of the organization's computer systems have application whitelisting software actively running?
3. Has the organization deployed an enterprise central management console for their anti-malware and whitelisting agents?
4. Are network filters and monitors in place on the organization's network to detect and block malicious code (especially at the organization's internet gateway)?
5. Are system business owners and executives regularly reviewing reports from the central management console(s) in order to respond properly to identified malware threats?

Standards References

CIS Critical Controls (v6.1):
2, 7, 8, 12

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-83

NIST 800-53 (rev4):
SI-3, SI-8

COBIT 5:
APO13, DSS05

ISO 27000:2013:
10.4

NIST Cybersecurity Framework:
DE.CM-4, DE.CM-5

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
5

HIPAA / HITECH:
HIPAA 164.308(a)(5)

Other Standards:
All current FIPS Publications (especially FIPS 140-2)