AuditScripts

Auditing Logging Systems

AuditScripts 5 Crucial Questions (v2.2)

SECURITY enclave

Auditing Logging Systems

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 logging systems, auditors should consider at a minimum asking the following questions:

1. Is logging enabled on all business sensitive systems in the organization?
2. Are all locally generated logs aggregated into a central log aggregation system?
3. Are all logs in the organization synchronized to a common, trusted time source (NTP)?
4. Are reports and alerts automatically generated as a result of the analysis of the centralized log files?
5. Are only authorized business users able to access local or centralized log files or reports?

Standards References

CIS Critical Controls (v6.1):
3, 4, 5, 6, 8, 11, 12, 13, 14, 16

NERC CIP (v5):
Not Applicable

NIST 800 Series:
NIST SP 800-21, 22
NIST SP 800-25, 29
NIST SP 800-32, 57, 111
NIST SP 800-130 – 133

NIST 800-53 (rev4):
IA-7, MP-4, MP-5, SC-8, SC-9, SC-11, SC-12, SC-13, SC-28

COBIT 5:
APO13, DSS05

ISO 27000:2013:
10.8, 10.9, 12.3

NIST Cybersecurity Framework:
PR.MA-1, PR.MA-2, PR.PT-1, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.CM-8, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.RP-1, RS.AN-1

IIA GTAGs:
Not Applicable

PCI DSS (v3.1):
2, 3, 4, 6, 7

HIPAA / HITECH:
HIPAA: 164.310(d)(1), 164.312(a)(1), 164.312(e)(1)
HITECH: 170.202, 170.205, 170.210

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