3.3.5 Correlate Audit Review, Analysis, and Reporting

Page Contents

Jump to...

3.5 Correlate Audit Review, Analysis, and Reporting

e

3.3.5. Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.

Guides

- NIST SP 800-92 - Guide to Computer Security Log Management
- SANS Institute - Successful SIEM and Log Management Strategies for Audit and Compliance
- Randy Franklin Smith's Ultimate Windows Security - February, 2017
- DFAR is Here, Are You Ready?
- DFARS Self-Reporting with Splunk

Sample Policy & Procedures

- Norfolk State University - Administrative Policy # 32 – 8 – 306 (2014) Audit Review, Analysis, and Reporting
- SANS Institute - Information Logging Standard

Videos

- BrightTALK - Log Management: Achieving Compliance Objectives
- BrightTALK - Universal Log Management – How Much Information is Too Much?
- BrightTALK - Rev up Your SIEM
- DFARS Self-Reporting with Splunk Enterprise

Example Tools

- Splunk
- EventTracker
- Rapid7
- AlienVault
- Logwatch

Additional Lessons Learned

- Audit Subsystem & Logwatch

Vendor Documentation

- EventTracker - FISMA-NIST SP 800-171 Solution Brief
- Tenable - NIST SP 800-171: Audit and Monitoring (3.3, 3.14)

How useful was this content?

Your Rating: Results: 9 rates