18. Logging

Thursday, August 15, 2024 2:31 PM

Process for Validating Stmt 18: Security Logging and Monitoring Activities

Overview:

The validation process for Stmt 18 focuses on ensuring that security logging and monitoring activities align with the CORE+ requirements. This includes verification of third-party vendor log monitoring, the audit log management process, detailed audit logging for sensitive data, and the collection of various types of logs across enterprise assets.

Step 1: Document Review and Policy Assessment

- **Obtain Documentation:**
  - Collect all relevant documentation, including logging and monitoring policies, third-party vendor agreements, and audit log management procedures.
  - Ensure that these documents clearly define the logging requirements, processes, and the responsibilities of all involved parties.
- **Evaluate Compliance with CORE+ Requirements:**
  - Review the documentation to ensure it aligns with the CORE+ requirements for logging and monitoring.
  - Ensure that the policies and procedures reflect current industry standards and best practices for security logging and monitoring.

Step 2: Verify Third-Party Vendor Log Monitoring (Stmt 18.1)

- **Vendor Contract Review:**
  - Obtain contracts or service level agreements (SLAs) with third-party vendors responsible for log monitoring.
  - Verify that the agreements include specific provisions for monitoring log activity and clearly outline the vendor's responsibilities.
- **Audit Vendor Activities:**
  - Request and review reports or logs from the third-party vendor to ensure they are actively monitoring log activity.
  - Check for documented procedures for how the vendor handles alerts, incidents, and reporting to the enterprise.
- **Interview Key Personnel:**
  - Conduct interviews with vendor representatives and internal stakeholders to confirm the implementation and effectiveness of the monitoring activities.

Step 3: Validate the Audit Log Management Process (Stmt 18.2)

- **Audit Log Management Review:**
  - Examine the enterprise's audit log management process to ensure it defines the logging requirements for all relevant systems.
  - Ensure that the process includes specific details about log retention periods, access controls, and procedures for reviewing logs.
- **Process Validation:**
  - Review logs from critical systems to verify that they are being managed according to the defined process.
  - Confirm that the audit log management process is regularly reviewed and updated to reflect changes in technology, compliance requirements, and enterprise needs.
- **Cross-Reference with Compliance Requirements:**
  - Ensure that the audit log management process aligns with regulatory requirements and industry standards.

Step 4: Review Detailed Audit Logging for Sensitive Data (Stmt 18.3)

- **Configuration Verification:**
  - Verify that detailed audit logging is configured for all enterprise assets containing sensitive data.
  - Ensure that logs capture key elements, including event source, date, username, timestamp, source addresses, and destination addresses.
- **Log Sample Analysis:**
  - Obtain a sample of audit logs from these assets to verify that the required elements are consistently captured.
  - Analyze the logs to ensure they contain sufficient detail to support forensic investigations if necessary.
- **Tool Configuration Review:**
  - Review the configuration of logging tools to confirm that they are set up to collect the required information.
  - Ensure that logs are stored securely and that access to them is restricted to authorized personnel only.

Step 5: Validate URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

- **Log Collection Review:**
  - Verify that URL request, DNS query, and command-line audit logs are being collected on enterprise assets where appropriate and supported.
  - Review system configurations to ensure that logging is enabled for these activities.
- **Log Sample Analysis:**
  - Analyze a sample of these logs to ensure that they are capturing relevant data.
  - Confirm that the logs provide sufficient information to identify potential security incidents.
- **Assess Log Integration:**
  - Ensure that these logs are integrated with the enterprise's centralized logging and monitoring system, allowing for comprehensive analysis and correlation.

Step 6: Review Collection of Service Provider Logs (Stmt 18.5)

- **Service Provider Log Assessment:**
  - Identify all third-party service providers that generate logs relevant to the enterprise's security posture.
  - Verify that logs from these providers are being collected, where supported.
- **Log Sample Analysis:**
  - Review samples of service provider logs to ensure they contain useful security information and are consistent with the enterprise's logging requirements.
  - Confirm that these logs are stored and managed according to the enterprise's audit log management process.
- **Collaboration with Providers:**
  - Engage with service providers to confirm that logs are being transmitted securely and that any issues related to log collection are promptly addressed.

Step 7: Reporting and Documentation

- **Compile Findings:**
  - Document the findings from each validation step, including any discrepancies or areas requiring improvement.
  - Provide recommendations for enhancing logging and monitoring activities based on the validation results.
- **Develop Action Plan:**
  - If gaps are identified, develop an action plan to address them. This may include updating policies, reconfiguring logging tools, or renegotiating vendor contracts.
  - Assign responsibilities and set deadlines for implementing corrective actions.
- **Final Report:**
  - Prepare a comprehensive report detailing the validation process, findings, and action plan.
  - Present the report to relevant stakeholders for review and approval.

Step 8: Continuous Monitoring and Review

- **Ongoing Monitoring:**
  - Establish a process for continuous monitoring of security logging and auditing activities to ensure ongoing compliance with CORE+ requirements.
  - Regularly review and update the audit log management process and vendor agreements as necessary.
- **Periodic Validation:**
  - Schedule periodic validations to ensure that the logging and monitoring activities continue to meet CORE+ standards and adapt to evolving threats and compliance requirements.

Tools

Thursday, August 15, 2024 2:33 PM

1. Document Review and Policy Assessment

- **Automation Tools:**
  - **Document Management Systems:** Use tools like SharePoint or Confluence to store and manage policies, procedures, and vendor contracts.
  - **Text Analysis:** Implement natural language processing (NLP) tools to automatically scan and identify relevant sections of documents for compliance with CORE+ requirements.
- **Automation Process:**
  - Set up automated workflows that trigger a review of documents when they are uploaded or updated.
  - Use NLP to highlight discrepancies or missing elements in policies and procedures, flagging them for manual review if necessary.

2. Third-Party Vendor Log Monitoring Validation (Stmt 18.1)

- **Automation Tools:**
  - **SIEM (Security Information and Event Management) Tools:** Use SIEM platforms like Splunk, QRadar, or Elastic Stack to aggregate, monitor, and analyze logs.
  - **API Integration:** Automate the collection and validation of logs from third-party vendors through APIs.
- **Automation Process:**
  - Configure the SIEM tool to automatically ingest and correlate logs from third-party vendors.
  - Set up automated alerts for any missing or inconsistent log entries.
  - Schedule regular automated audits of vendor log data against SLAs and compliance requirements.

3. Audit Log Management Process Validation (Stmt 18.2)

- **Automation Tools:**
  - **Log Management Tools:** Use centralized log management systems like LogRhythm or Graylog to enforce and monitor logging requirements.
  - **Policy Compliance Checkers:** Deploy tools that can automatically check log management processes against defined policies and compliance standards.
- **Automation Process:**
  - Automate log collection, retention, and access controls using a centralized log management system.
  - Configure periodic automated checks to validate compliance with log management policies and identify any deviations.

4. Detailed Audit Logging for Sensitive Data (Stmt 18.3)

- **Automation Tools:**
  - **SIEM and Log Analysis Tools:** Use SIEM tools to automatically capture and analyze logs containing sensitive data.
  - **Compliance Monitoring:** Implement tools like Tripwire or Varonis to ensure that logs capture required elements like event source, date, username, etc.
- **Automation Process:**
  - Set up the SIEM tool to automatically collect detailed logs from assets containing sensitive data.
  - Automate the validation process by configuring the SIEM to check for the presence of required elements (event source, date, username, etc.) in the logs.
  - Use automated scripts to regularly sample and analyze logs, ensuring they meet forensic investigation requirements.

5. URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

- **Automation Tools:**
  - **Endpoint Detection and Response (EDR) Tools:** Use EDR tools like CrowdStrike, Carbon Black, or Microsoft Defender to automatically capture URL requests, DNS queries, and command-line activities.
  - **Network Monitoring Tools:** Implement tools like Zeek (formerly Bro) or Suricata for DNS and network traffic analysis.
- **Automation Process:**
  - Automate the collection of URL request, DNS query, and command-line logs using EDR and network monitoring tools.
  - Set up automated correlation and analysis within the SIEM to identify potential security incidents.
  - Implement automated alerts for any suspicious activities detected in these logs.

6. Service Provider Logs Collection (Stmt 18.5)

- **Automation Tools:**
  - **Cloud Security Tools:** Use tools like AWS CloudTrail, Google Cloud Logging, or Azure Monitor to automatically collect logs from cloud service providers.
  - **API Integration:** Leverage APIs to automate the collection of logs from third-party service providers.
- **Automation Process:**
  - Configure cloud security tools to automatically collect and store service provider logs.
  - Set up periodic automated checks to ensure that all required logs are being collected and that they align with enterprise logging requirements.
  - Automate the integration of these logs into the centralized log management system or SIEM for analysis and reporting.

7. Reporting and Documentation

- **Automation Tools:**
  - **Reporting Tools:** Use automated reporting tools like Power BI, Tableau, or custom scripts to generate compliance reports.
  - **Document Automation:** Implement document automation platforms to generate and update reports based on the analysis.
- **Automation Process:**
  - Configure reporting tools to automatically generate compliance reports based on the validation results from SIEM, EDR, and log management systems.
  - Set up automated workflows to compile and distribute these reports to relevant stakeholders on a regular schedule.

8. Continuous Monitoring and Review

- **Automation Tools:**
  - **SIEM and Continuous Monitoring Tools:** Use SIEM tools with continuous monitoring capabilities to automate the ongoing validation of security logging and monitoring activities.
  - **Automated Alerts:** Implement automated alerting mechanisms for any deviations or failures in logging processes.
- **Automation Process:**
  - Automate continuous monitoring by configuring the SIEM to track compliance with logging and monitoring requirements in real time.
  - Set up automated alerts and notifications for any issues, such as missing logs, failed log transmissions, or non-compliance with policies.
  - Schedule regular automated reviews to validate that logging and monitoring activities continue to meet CORE+ requirements.

9. Integration and Orchestration

- **Automation Tools:**
  - **SOAR (Security Orchestration, Automation, and Response) Tools:** Use SOAR platforms like Palo Alto Cortex XSOAR or Splunk Phantom to automate and orchestrate the entire validation process.
  - **Workflow Automation:** Implement workflow automation tools like Zapier or ServiceNow to connect different systems and automate processes.
- **Automation Process:**
  - Use SOAR tools to automate the end-to-end validation process, integrating data collection, analysis, reporting, and alerting.
  - Configure workflows that trigger actions based on specific events, such as generating reports or initiating corrective actions.

Resources

Thursday, August 15, 2024 2:33 PM

Policy and Procedure	Review Security Monitoring policy and procedure to validate the organization has a formal Security Monitoring policy and procedure	Security Monitoring policy and procedure	The organization has a formal Security Monitoring policy and procedure detailing the requirements and implementation for logs to be collected and analyzed, responsibilities for responding to alerts, and log retention of at least 1 year.
Log Aggregation/Correlation	Interview administrator to validate that the organization utilizes a Log Aggregator to collect logs Review Log Aggregator log sources Review sample logging alert	Log Aggregator log sources Sample logging alert	The organization utilizes a Log Aggregator or SIEM to collect logs from production servers and network devices, including dom ain controllers and firewalls. Logs are analyzed and alerts are generated on anomalous activity.
File Integrity Monitoring	Interview administrator to verify the organization has implemented a file integrity monitoring solution		The organization has implemented a file integrity monitoring solution
System Health Monitoring	Interview administrator to verify the organization has implemented system health monitoring		The organization has implemented system health monitoring, with automatic alerting including disk space, memory, and up/down status.


ASD - Best practices ...


LME Fact Sheet - Fi...


LME Frequentl...

PowerShell

Thursday, August 15, 2024 2:35 PM

1. Third-Party Vendor Log Monitoring (Stmt 18.1)

PowerShell might not directly validate third-party vendor log monitoring, but it can help automate the process of verifying log ingestion and integration from these vendors.

Example Script: Check Log Integration

```
# Check if logs from a third-party vendor are being ingested into a SIEM system
$logSource = "VendorName"
$siemServer = "SIEMServerAddress"

# Define the log source
$logSourceCheck = Get-WinEvent -LogName "Application" | Where-Object { $_.ProviderName -eq $logSource }

# Check if logs are present
if ($logSourceCheck) {
    Write-Output "Logs from $logSource are present."
} else {
    Write-Output "No logs from $logSource found."
}

# Optional: Query SIEM API for more detailed status
```

2. Audit Log Management Process (Stmt 18.2)

Automate the validation of log management by checking log retention, access controls, and compliance settings.

Example Script: Check Log Retention Policy

```
# Example for checking log retention settings on Windows Event Logs
$logRetention = Get-WinEvent -ListLog * | Where-Object { $_.LogName -eq "Application" } | Select-Object -Property LogName, Retention
Write-Output "Log Retention Settings:"
$logRetention
```

3. Detailed Audit Logging for Sensitive Data (Stmt 18.3)

Validate the configuration and content of audit logs to ensure they include required details.

Example Script: Check for Detailed Logging

```
# Check if detailed audit logging is enabled for a specific log source
$logSource = "Application"
$logDetails = Get-WinEvent -LogName $logSource | Select-Object -First 10
Write-Output "Recent log entries from $logSource:"
$logDetails | Format-List TimeCreated, ProviderName, Id, Message
```

4. URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

Automate the collection and analysis of URL request, DNS query, and command-line logs.

Example Script: Check Command-Line Audit Logs

```
# Ensure command-line auditing is enabled in Windows
$auditingStatus = Get-ItemProperty -Path "HKLM:\Software\Policies\Microsoft\Windows\System" -Name "EnableCommandLineAuditing"
Write-Output "Command-Line Auditing Enabled: $($auditingStatus.EnableCommandLineAuditing)"

Example Script: Check DNS Query Logs
# Example for DNS query logging (requires DNS server access)
$dnsLogPath = "C:\DNSLogs"
$dnsLogs = Get-ChildItem -Path $dnsLogPath -Filter "*.log"
Write-Output "DNS Query Logs:"
$dnsLogs | ForEach-Object { Get-Content $_.FullName | Select-Object -First 10 }
```

5. Service Provider Logs Collection (Stmt 18.5)

Automate the validation of log collection from cloud service providers.

Example Script: Check Cloud Logs Collection (AWS Example)

```
# Requires AWS Tools for PowerShell
Import-Module AWSPowerShell

# Check if CloudTrail is enabled for AWS
$trailStatus = Get-CTTrail
Write-Output "CloudTrail Status:"
$trailStatus
```

Integration and Orchestration

Example Script: Integrate with SIEM

```
# Example for querying a SIEM API for log data
$siemApiUrl = " https://siem.example.com/api/logs"
$response = Invoke-RestMethod -Uri $siemApiUrl -Method Get -Headers @{Authorization = "Bearer YourToken"}
Write-Output "SIEM Logs:"
$response

Example Script: Automate Report Generation
# Generate a simple compliance report
$report = @"
Compliance Report:
==================
- Third-Party Vendor Log Monitoring: Validated
- Audit Log Management: Verified
- Detailed Logging: Enabled
- URL/DNS/Command-Line Logs: Collected
```

```
- Service Provider Logs: Present
"@

$reportPath = "C:\Reports\ComplianceReport.txt"
$report | Out-File -FilePath $reportPath
Write-Output "Report Generated at $reportPath"
```

Questions

Thursday, October 10, 2024 4:10 PM

Step 1: Document Review and Policy Assessment

1. **Obtain Documentation**:
    - Q1.1: Have all relevant documents, including logging and monitoring policies, third-party vendor agreements, and audit log management procedures, been collected?
    - Q1.2: Do these documents clearly define the logging requirements, processes, and responsibilities of all involved parties?
2. **Evaluate Compliance with CORE+ Requirements**:
    - Q1.3: Does the documentation align with CORE+ requirements for logging and monitoring?
    - Q1.4: Do the policies and procedures reflect current industry standards and best practices for security logging and monitoring?

Step 2: Verify Third-Party Vendor Log Monitoring (Stmt 18.1)

1. **Vendor Contract Review**:
    - Q2.1: Are contracts or SLAs with third-party vendors responsible for log monitoring available for review?
    - Q2.2: Do these agreements include specific provisions for monitoring log activity and clearly outline the vendor's responsibilities?
2. **Audit Vendor Activities**:
    - Q2.3: Are reports or logs from the third-party vendor reviewed regularly to ensure active monitoring?
    - Q2.4: Are documented procedures in place for how the vendor handles alerts, incidents, and reporting?
3. **Interview Key Personnel**:
    - Q2.5: Are interviews conducted with vendor representatives and internal stakeholders to confirm the effectiveness of monitoring activities?

Step 3: Validate the Audit Log Management Process (Stmt 18.2)

1. **Audit Log Management Review**:
    - Q3.1: Does the enterprise have a defined audit log management process for all relevant systems?
    - Q3.2: Does the process specify log retention periods, access controls, and procedures for reviewing logs?
2. **Process Validation**:
    - Q3.3: Are logs from critical systems reviewed to verify they are managed according to the defined process?
    - Q3.4: Is the audit log management process regularly reviewed and updated to reflect technological and compliance changes?
3. **Cross-Reference with Compliance Requirements**:
    - Q3.5: Does the audit log management process align with regulatory requirements and industry standards?

Step 4: Review Detailed Audit Logging for Sensitive Data (Stmt 18.3)

1. **Configuration Verification**:
    - Q4.1: Is detailed audit logging configured for all assets containing

sensitive data?
    - Q4.2: Do logs capture key elements such as event source, date, username, timestamp, source addresses, and destination addresses?
2. **Log Sample Analysis**:
    - Q4.3: Are log samples from sensitive assets reviewed to verify that the required elements are consistently captured?
    - Q4.4: Do the logs contain sufficient detail to support forensic investigations if necessary?
3. **Tool Configuration Review**:
    - Q4.5: Are logging tools configured correctly to collect the required information?
    - Q4.6: Are logs stored securely, and is access restricted to authorized personnel only?

Step 5: Validate URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

1. **Log Collection Review**:
    - Q5.1: Are URL request, DNS query, and command-line audit logs collected where appropriate and supported?
    - Q5.2: Are system configurations reviewed to ensure logging is enabled for these activities?
2. **Log Sample Analysis**:
    - Q5.3: Are samples of these logs analyzed to ensure relevant data is captured?
    - Q5.4: Do the logs provide sufficient information to identify potential security incidents?
3. **Assess Log Integration**:
    - Q5.5: Are these logs integrated with the enterprise's centralized logging and monitoring system for comprehensive analysis?

Step 6: Review Collection of Service Provider Logs (Stmt 18.5)

1. **Service Provider Log Assessment**:
    - Q6.1: Are all third-party service providers that generate relevant logs identified?
    - Q6.2: Are logs from these providers being collected, where supported?
2. **Log Sample Analysis**:
    - Q6.3: Are samples of service provider logs reviewed to ensure they contain useful security information consistent with the enterprise's logging requirements?
    - Q6.4: Are these logs stored and managed according to the enterprise's audit log management process?
3. **Collaboration with Providers**:
    - Q6.5: Are service providers engaged to confirm secure transmission of logs and address any log collection issues promptly?

Step 7: Reporting and Documentation

1. **Compile Findings**:
    - Q7.1: Are findings from each validation step documented, including any discrepancies or areas requiring improvement?
    - Q7.2: Are recommendations for enhancing logging and monitoring activities based on validation results provided?

2. **Develop Action Plan**:
    - Q7.3: If gaps are identified, is an action plan developed to address them, including updating policies or reconfiguring logging tools?
    - Q7.4: Are responsibilities assigned, and deadlines set for implementing corrective actions?
3. **Final Report**:
    - Q7.5: Is a comprehensive report prepared detailing the validation process, findings, and action plan?
    - Q7.6: Is the report presented to relevant stakeholders for review and approval?

Step 8: Continuous Monitoring and Review

1. **Ongoing Monitoring**:
    - Q8.1: Is there a process for continuous monitoring of security logging and auditing activities to ensure compliance with CORE+ requirements?
    - Q8.2: Are audit log management processes and vendor agreements regularly reviewed and updated?
2. **Periodic Validation**:
    - Q8.3: Are periodic validations scheduled to ensure logging and monitoring activities meet CORE+ standards and adapt to evolving threats?
    - Q8.4: Are processes updated based on the results of periodic validation and compliance requirements?

Answers

Thursday, October 10, 2024 4:11 PM

Step 1: Document Review and Policy Assessment

1. **Obtain Documentation**:
    - **Positive Response**: All relevant documentation is collected, comprehensive, and up-to-date.
    - **Negative Response**: Some or all relevant documentation is missing, outdated, or incomplete.
2. **Evaluate Compliance with CORE+ Requirements**:
    - **Positive Response**: Documentation aligns with CORE+ requirements and reflects industry best practices.
    - **Negative Response**: Documentation does not meet CORE+ requirements, lacks detail, or fails to align with best practices.

Step 2: Verify Third-Party Vendor Log Monitoring (Stmt 18.1)

1. **Vendor Contract Review**:
    - **Positive Response**: Contracts include specific provisions for monitoring log activity, and vendor responsibilities are clearly defined.
    - **Negative Response**: Contracts lack provisions for log monitoring, or vendor responsibilities are not clearly outlined.
2. **Audit Vendor Activities**:
    - **Positive Response**: Reports and logs from third-party vendors show active monitoring, with clear procedures for handling incidents.
    - **Negative Response**: Reports or logs are missing, incomplete, or indicate that monitoring is not active or consistent.
3. **Interview Key Personnel**:
    - **Positive Response**: Interviews confirm that monitoring activities are implemented effectively and are aligned with policies.
    - **Negative Response**: Interviews reveal gaps in implementation, lack of clarity, or inconsistencies in monitoring practices.

Step 3: Validate the Audit Log Management Process (Stmt 18.2)

1. **Audit Log Management Review**:
    - **Positive Response**: The audit log management process is well-defined, specifying log retention periods and access controls.
    - **Negative Response**: The process is vague, lacks essential details (e.g., retention periods, access controls), or is not documented.
2. **Process Validation**:
    - **Positive Response**: Logs from critical systems are managed according to the defined process, and regular reviews are conducted.
    - **Negative Response**: Logs are not managed as per the defined process, or reviews are irregular or not performed.
3. **Cross-Reference with Compliance Requirements**:
    - **Positive Response**: The audit log management process aligns with regulatory requirements and industry standards.
    - **Negative Response**: The process does not meet regulatory requirements or industry standards.

Step 4: Review Detailed Audit Logging for Sensitive Data (Stmt 18.3)

1. **Configuration Verification**:
    - **Positive Response**: Detailed audit logging is enabled for all assets with sensitive data, capturing all key elements.
    - **Negative Response**: Logging is not enabled for all assets or is missing key elements such as timestamps or source addresses.
2. **Log Sample Analysis**:
    - **Positive Response**: Log samples show consistent capture of all required elements, with sufficient detail for investigations.
    - **Negative Response**: Log samples are inconsistent or lack sufficient detail for forensic investigations.
3. **Tool Configuration Review**:
    - **Positive Response**: Logging tools are properly configured, storing logs securely with restricted access.
    - **Negative Response**: Tools are misconfigured, or logs are not stored securely, with access controls not properly enforced.

Step 5: Validate URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

1. **Log Collection Review**:
    - **Positive Response**: Logs are being collected for URL requests, DNS queries, and command-line activities where appropriate.
    - **Negative Response**: Logs are missing, or logging is not enabled for these activities as required.
2. **Log Sample Analysis**:
    - **Positive Response**: Log samples capture relevant data, providing sufficient information to identify security incidents.
    - **Negative Response**: Logs do not capture enough data, or samples are incomplete, hindering incident identification.
3. **Assess Log Integration**:
    - **Positive Response**: Logs are integrated with the centralized monitoring system, enabling comprehensive analysis.
    - **Negative Response**: Logs are not integrated, or integration is incomplete, limiting the monitoring system's effectiveness.

Step 6: Review Collection of Service Provider Logs (Stmt 18.5)

1. **Service Provider Log Assessment**:
    - **Positive Response**: All relevant service providers have been identified, and their logs are collected according to requirements.
    - **Negative Response**: Not all providers are identified, or their logs are not being collected as required.
2. **Log Sample Analysis**:
    - **Positive Response**: Samples of service provider logs meet enterprise logging requirements and provide useful security information.
    - **Negative Response**: Logs do not meet requirements or lack the necessary detail for effective monitoring.
3. **Collaboration with Providers**:
    - **Positive Response**: Providers transmit logs securely, and any issues with log collection are promptly addressed.
    - **Negative Response**: Providers do not ensure secure log transmission,

or issues with log collection remain unresolved.

Step 7: Reporting and Documentation

1. **Compile Findings**:
    - **Positive Response**: Findings are thoroughly documented, with discrepancies clearly identified and recommendations provided.
    - **Negative Response**: Documentation is incomplete, and discrepancies or recommendations are not clearly outlined.
2. **Develop Action Plan**:
    - **Positive Response**: An action plan with assigned responsibilities and deadlines is developed for addressing gaps.
    - **Negative Response**: No action plan is created, or it lacks clarity, responsibilities, or deadlines.
3. **Final Report**:
    - **Positive Response**: A comprehensive report detailing the process, findings, and action plan is presented to stakeholders.
    - **Negative Response**: The report is incomplete or not presented for stakeholder review and approval.

Step 8: Continuous Monitoring and Review

1. **Ongoing Monitoring**:
    - **Positive Response**: A process for continuous monitoring is established, ensuring compliance with CORE+ requirements.
    - **Negative Response**: Monitoring is either not continuous or does not adequately cover all areas required by CORE+.
2. **Periodic Validation**:
    - **Positive Response**: Validations are scheduled periodically to adapt to evolving threats and compliance requirements.
    - **Negative Response**: No periodic validations are scheduled, or validations are not updated based on new threats or regulations.

Checklist

Thursday, October 10, 2024 4:12 PM

Compliance Checklist for Logging and Monitoring

Step 1: Document Review and Policy Assessment

- All relevant documentation (logging policies, third-party agreements, audit log management procedures) is collected and up-to-date.
- Policies and procedures clearly define logging requirements, processes, and responsibilities.
- Documentation aligns with CORE+ requirements and reflects current industry best practices.

Step 2: Verify Third-Party Vendor Log Monitoring (Stmt 18.1)

- Contracts or SLAs with third-party vendors include provisions for monitoring log activity and clearly outline responsibilities.
- Reports or logs from third-party vendors are actively monitored and reviewed.
- Documented procedures are in place for how vendors handle alerts, incidents, and reporting.
- Interviews confirm the implementation and effectiveness of third-party monitoring activities.

Step 3: Validate the Audit Log Management Process (Stmt 18.2)

- The audit log management process is documented and defines logging requirements, retention periods, and access controls.
- Logs from critical systems are managed according to the defined process and are reviewed regularly.
- The audit log management process aligns with regulatory requirements and industry standards.

Step 4: Review Detailed Audit Logging for Sensitive Data (Stmt 18.3)

- Detailed audit logging is configured for all enterprise assets containing sensitive data.
- Logs capture essential elements (e.g., event source, date, username, timestamp, source/destination addresses).
- Log samples show consistent capture of required elements and sufficient detail for investigations.
- Logging tools are configured correctly, with logs stored securely and access restricted to authorized personnel.

Step 5: Validate URL Request, DNS Query, and Command-Line Audit Logs (Stmt 18.4)

- URL request, DNS query, and command-line logs are collected where appropriate.
- System configurations are reviewed to ensure these activities are logged.
- Log samples are analyzed and provide sufficient information for identifying potential incidents.
- Logs are integrated with the centralized logging and monitoring system.

Step 6: Review Collection of Service Provider Logs (Stmt 18.5)

- Third-party service providers that generate relevant logs are identified.
- Logs from these providers are collected and assessed for compliance with enterprise requirements.
- Samples of service provider logs meet enterprise standards and provide necessary

security information.
- Service providers securely transmit logs, and any issues are promptly resolved.

Step 7: Reporting and Documentation

- Findings from each validation step are documented, with discrepancies and recommendations clearly outlined.
- An action plan with responsibilities and deadlines is developed for addressing identified gaps.
- A comprehensive report detailing the validation process, findings, and action plan is presented to stakeholders.

Step 8: Continuous Monitoring and Review

- A process for continuous monitoring of logging and auditing activities is established.
- The audit log management process and vendor agreements are reviewed and updated regularly.
- Periodic validations are scheduled to ensure ongoing compliance with CORE+ standards and to adapt to evolving threats.

Additional Considerations

- Are all findings and compliance statuses documented and reviewed by relevant stakeholders?
- Are corrective actions and updates implemented promptly when discrepancies are identified?
- Is training provided to personnel involved in logging and monitoring processes to ensure adherence to policies?

Notes

Tuesday, September 3, 2024 1:33 PM

1. Log Generation:
- Enable audit logging on all critical systems, applications, and network devices to capture security-relevant events, including access attempts, configuration changes, and user activities.

2. Log Storage:
- Securely store audit logs in a centralized log management system to prevent tampering and unauthorized access.
- Implement encryption and access controls to protect the confidentiality and integrity of stored logs.

3. Retention Period:
- Retain audit logs for a minimum period of 90 days to comply with regulatory, legal, and business requirements.
- Extend retention periods for logs related to significant security incidents or ongoing investigations as needed.

4. Log Review and Monitoring:
- Regularly review and analyze audit logs to detect suspicious activities and potential security incidents.
- Implement automated tools and processes to assist in log analysis and alerting.

5. Disposition:
- Securely dispose of audit logs after the retention period has expired, ensuring that deleted logs cannot be recovered or reconstructed.