Monitoring

Thursday, August 15, 2024 12:54 PM

Comprehensive Process for Validating Stmt 17: Anomalous Activity Monitoring

This process will ensure that each CORE+ statement related to anomalous activity monitoring is validated thoroughly. The validation process will include a review of documentation, system configuration, logs, and interviews with relevant personnel.

Step 1: Understand the Requirements

- **Review Guidelines and Standards:** Begin by reviewing relevant guidelines, such as NIST SP 800-137, CIS Controls, and FFIEC IT Examination Handbook. Ensure a deep understanding of what is expected for each CORE+ statement.
- **Identify Key Assets:** Identify the key assets, such as firewalls, intrusion detection/prevention systems (IDS/IPS), SIEM tools, network devices, and wireless access points, that will be involved in monitoring anomalous activity.

Step 2: Documentation Review

- **Review Security Policies and Procedures:**
  - Validate that documented procedures exist for each component listed under Stmt 17.
  - Ensure policies are up-to-date and include detailed instructions for monitoring network traffic, log collection, and event alerting.

Step 3: System Configuration Validation

- **Stmt 17.1 & 17.2 - Monitoring Incoming and Outgoing Network Traffic:**
  - Verify that network monitoring tools (e.g., IDS/IPS, firewalls) are configured to monitor both incoming and outgoing traffic.
  - Check that network traffic logs are being generated and stored.
- **Stmt 17.3 - Monitoring for Insider Malicious Activity:**
  - Review tools and techniques used to monitor insider threats, such as user behavior analytics (UBA) tools.
  - Validate that alerts are generated for anomalous insider activities.
- **Stmt 17.4 & 17.5 - Logs Collected from Key Systems and Analyzed:**
  - Verify that logs are collected from critical systems, including servers, firewalls, and endpoint security solutions.
  - Ensure there is a process for regular log analysis, and review past analysis reports.
- **Stmt 17.6 - Centralized Security Event Alerting and Logging:**
  - Confirm that a SIEM or equivalent tool is in place for centralized log collection and correlation.
  - Review the configuration of the SIEM to ensure it covers all enterprise assets.
- **Stmt 17.7 - Tuning Security Event Alerting Thresholds:**
  - Check the process for tuning alert thresholds in the SIEM.
  - Verify that the tuning is done at least monthly or more frequently as needed.
- **Stmt 17.8 - Port Monitoring:**
  - Validate that port monitoring tools are in use and configured to detect unauthorized network connections.
- **Stmt 17.9 - Appropriate Controls Over Wired and Wireless Networks:**
  - Review the configuration of network controls, including Network Access Control (NAC) for wired and wireless networks.
  - Ensure that only authorized devices can connect to the network.
- **Stmt 17.10 - Host-Based Intrusion Detection:**
  - Verify that a host-based IDS is deployed on enterprise assets.
  - Confirm that the IDS is actively monitoring and generating alerts.
- **Stmt 17.11 - Traffic Filtering Between Network Segments:**
  - Check that traffic filtering mechanisms (e.g., firewalls, VLANs) are in place between network segments.
  - Ensure that appropriate rules are configured to filter traffic.
- **Stmt 17.12 - Application Layer Filtering:**
  - Verify the presence of an application layer filtering solution, such as a proxy or application layer firewall.
  - Review the rules configured to filter traffic at the application layer.
- **Stmt 17.13 - Encryption on Wireless Networks:**
  - Ensure that encryption protocols (e.g., WPA2, WPA3) are in use for wireless networks.
  - Review the configuration to confirm that encryption is properly implemented.
- **Stmt 17.14 - Wireless Networks Segmentation:**
  - Verify that wireless networks are segmented appropriately to separate guest access from internal network access.
  - Review network diagrams to confirm proper segmentation.
- **Stmt 17.15 - Authentication Standards for Wireless Networks:**
  - Check that strong authentication mechanisms, such as 802.1x, are in place for wireless networks.
  - Validate the use of complex passwords and the proper implementation of authentication protocols.

Step 4: Interview Relevant Personnel

- **Speak with IT and Security Teams:** Interview personnel responsible for network monitoring, log analysis, and incident response. Ensure they are aware of and following the documented procedures.
- **Confirm Training and Awareness:** Verify that staff involved in monitoring and responding to anomalous activities have received proper training.

Step 5: Testing and Validation

- **Conduct Simulated Attacks:** Perform penetration testing and/or red team exercises to simulate attacks and insider threats. Validate that monitoring systems detect and alert on these activities.
- **Review Logs and Alerts:** Select a sample of logs and alerts from the SIEM and other monitoring tools to confirm that anomalous activities are detected and responded to appropriately.
- **Assess Tuning Effectiveness:** Review the effectiveness of tuning practices by examining the rate of false positives and the speed of detecting real threats.

Step 6: Reporting

- **Document Findings:** Prepare a detailed report documenting the validation process, findings, and any gaps identified.
- **Recommendations:** Provide recommendations for addressing any gaps or weaknesses in the monitoring process.
- **Follow-Up:** Establish a process for continuous monitoring and regular revalidation of the components under Stmt 17.

Tools

Thursday, August 15, 2024 1:10 PM

1. Network Traffic Monitoring Tools
- **Wireshark**: A network protocol analyzer that can capture and interactively browse traffic running on a computer network.
- **Zeek (formerly Bro)**: A powerful network analysis framework that focuses on network security monitoring.
- **Snort**: An open-source network intrusion detection and prevention system (IDS/IPS) that can analyze network traffic in real time.

2. Insider Malicious Activity Monitoring Tools
- **Varonis**: A data security platform that provides insights into user behavior and monitors for insider threats.
- **ObserveIT**: Provides user activity monitoring and insider threat detection by tracking user activity on endpoints.
- **Splunk UBA (User Behavior Analytics)**: A machine learning-driven solution that detects insider threats by analyzing user behavior.

3. Log Collection and Analysis Tools
- **Graylog**: An open-source log management tool that allows centralized log collection and analysis.
- **LogRhythm**: A security intelligence platform that integrates log collection, analysis, and SIEM.
- **Fluentd**: An open-source data collector that unifies log data collection and consumption.

4. Security Information and Event Management (SIEM) Tools
- **Splunk Enterprise Security**: Provides comprehensive monitoring, threat detection, and incident response capabilities.
- **IBM QRadar**: A SIEM solution that provides real-time monitoring, log management, and automated threat detection.
- **ArcSight**: A SIEM platform that provides log management, advanced threat detection, and security analytics.

5. Port Monitoring Tools
- **Nmap**: A network scanning tool that identifies open ports, services running, and other network devices.
- **NetFlow Analyzer**: Provides real-time network traffic monitoring, including port usage analysis.
- **SolarWinds Network Performance Monitor**: Monitors network traffic and tracks port usage across devices.

6. Network Access Control (NAC) Tools
- **Cisco Identity Services Engine (ISE)**: Provides secure access control across wired, wireless, and VPN connections.
- **Aruba ClearPass**: A NAC solution that offers advanced policy management and secure network access.
- **FortiNAC**: Provides visibility, control, and automated response to network access violations.

7. Host-Based Intrusion Detection Systems (HIDS)
- **OSSEC**: An open-source HIDS that monitors file integrity, rootkit detection, and log analysis on host systems.
- **Tripwire**: A commercial HIDS solution that monitors file integrity and provides alerts for unauthorized changes.
- **AIDE (Advanced Intrusion Detection Environment)**: An open-source HIDS that monitors file integrity and system configuration changes.

8. Traffic Filtering and Segmentation Tools
- **pfSense**: An open-source firewall/router software that provides traffic filtering and network segmentation.
- **Cisco ASA (Adaptive Security Appliance)**: A firewall solution that provides advanced traffic filtering and segmentation.
- **FortiGate**: A next-generation firewall that provides comprehensive network protection, including traffic filtering and segmentation.

9. Application Layer Filtering Tools
- **Squid Proxy**: An open-source proxy server that provides content filtering and application layer traffic control.
- **Zscaler**: A cloud-based web security solution that provides application layer filtering and secure web gateway services.
- **Palo Alto Networks Next-Generation Firewall**: Provides application layer filtering along with advanced threat prevention.

10. Wireless Network Encryption and Authentication Tools
- **AirMagnet WiFi Analyzer**: A wireless network troubleshooting tool that analyzes Wi-Fi networks, including encryption settings.
- **Ekahau Wi-Fi Design**: Provides tools for designing and validating Wi-Fi networks, including encryption and authentication standards.
- **WPA2 Enterprise with 802.1x**: Protocols that ensure secure authentication for wireless networks by enforcing user and device credentials.

11. Wireless Network Segmentation Tools
- **Cisco Wireless LAN Controller (WLC)**: Manages wireless network segmentation, including guest and internal network separation.
- **Meraki Dashboard**: Provides cloud-based control over wireless networks, allowing easy segmentation between different SSIDs.
- **Ubiquiti UniFi Controller**: Manages UniFi devices and allows the segmentation of wireless networks into separate VLANs.

12. Log Aggregation and Correlation Tools
- **ELK Stack (Elasticsearch, Logstash, Kibana)**: A powerful open-source log aggregation and analysis suite.
- **Sumo Logic**: A cloud-native log management and security analytics service that provides real-time insights and correlation.
- **Rapid7 InsightIDR**: A SIEM tool that combines log aggregation with user behavior analytics and endpoint detection.

13. Traffic Filtering Between Network Segments Tools
- **Cisco ASA**: Manages and filters traffic between different network segments using advanced access control lists (ACLs).
- **FortiGate NGFW**: Provides segmentation and traffic filtering between different network segments or security zones.
- **Palo Alto Networks Firewall**: Offers granular traffic filtering between network segments, including Layer 7 application control.

14. Log Management Tools
- **Splunk**: An industry-leading log management solution that allows for comprehensive search, monitoring, and analysis of machine data.
- **AlienVault USM**: Provides unified security management, including log management, SIEM, and intrusion detection.
- **ManageEngine EventLog Analyzer**: Offers log management, network log analysis, and auditing capabilities.

15. Encryption Tools for Wireless Networks
- **OpenSSL**: Provides a toolkit for implementing secure communications, including encryption protocols for Wi-Fi networks.
- **Wi-Fi Protected Access (WPA3)**: The latest Wi-Fi encryption standard offering enhanced protection against unauthorized access.
- **RADIUS (Remote Authentication Dial-In User Service)**: Provides secure authentication and encryption services for wireless networks.

16. SIEM Tuning Tools
- **Splunk Machine Learning Toolkit**: Provides machine learning capabilities for tuning SIEM alert thresholds.
- **QRadar Advisor with Watson**: Uses AI to help tune SIEM rules and reduce false positives.
- **ArcSight Management Center**: Centralizes the management and tuning of ArcSight SIEM deployments, including alert thresholds.

17. Wireless Network Management Tools

- **AirMagnet Survey**: Analyzes and validates the configuration of wireless networks, including segmentation and security settings.
- **Cisco Prime Infrastructure**: Manages wireless network configurations, security, and segmentation.
- **Ruckus ZoneDirector**: Provides centralized management and monitoring of wireless networks, ensuring proper segmentation and authentication.

18. Event Log Analysis Tools

- **SolarWinds Log & Event Manager**: Provides real-time event log analysis and correlation for network security monitoring.
- **Splunk**: Powerful search and analysis capabilities for analyzing event logs and detecting anomalies.
- **Loggly**: A cloud-based log analysis tool that helps in monitoring and analyzing event logs from various sources.

19. Authentication Tools for Wireless Networks

- **Cisco ISE (Identity Services Engine)**: Provides secure authentication and authorization services for wireless networks.
- **FreeRADIUS**: An open-source RADIUS server that provides strong authentication for wireless networks.
- **ClearBox**: A RADIUS server and management tool that enforces 802.1x authentication on wireless networks.

Resources

Thursday, August 15, 2024 1:11 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 domain 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.

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Management performs security monitoring for the network and all critical systems and applications; ☐ Systems to detect or prevent unauthorized network access; ☐ Network vulnerability assessments and penetration tests; ☐ Ability to detect and prevent the unauthorized removal of data from the network; ☐ Ability to detect and respond to anomalous activity; ☐ Processes for implementing and managing network security devices; ☐ Log monitoring program; ☐ Advanced encryption standards (AES) to encrypt wireless data in transit is mandatory; ☐ Wireless configuration and monitoring; ☐ Ability to prevent or detect unauthorized devices and unauthorized software.	☐ Management performs security monitoring for the network and all critical systems and applications; ☐ Systems to detect or prevent unauthorized network access; ☐ Network vulnerability assessments and penetration tests; ☐ Ability to detect and prevent the unauthorized removal of data from the network; ☐ Ability to detect and respond to anomalous activity; ☐ Processes for implementing and managing network security devices; ☐ Log monitoring program; ☐ Advanced encryption standards (AES) to encrypt wireless data in transit is mandatory; ☐ No wireless configuration and monitoring; ☐ No ability to comprehensively prevent or detect unauthorized devices and unauthorized software.	☐ Management performs security monitoring the network and some but not all critical systems and applications; ☐ No systems to detect or prevent unauthorized network access; ☐ No network vulnerability assessments and penetration tests; ☐ No ability to detect and prevent the unauthorized removal of data from the network; ☐ No ability to detect and respond to anomalous activity; ☐ No processes for implementing and managing network security devices; ☐ No log monitoring program; ☐ No wireless configuration and monitoring; ☐ Advanced encryption standards (AES) to encrypt wireless data in transit is not mandatory; ☐ No wireless configuration and monitoring; ☐ No ability to prevent or detect unauthorized devices and unauthorized software.	☐ Management does not perform security monitoring; ☐ No systems to detect or prevent unauthorized network access; ☐ No network vulnerability assessments and penetration tests; ☐ No ability to detect and prevent the unauthorized removal of data from the network; ☐ No ability to detect and respond to anomalous activity; ☐ No processes for implementing and managing network security devices; ☐ No log monitoring program; ☐ No wireless configuration and monitoring; ☐ Advanced encryption standards (AES) to encrypt wireless data in transit is not mandatory; ☐ No wireless configuration and monitoring; ☐ No ability to prevent or detect unauthorized devices and unauthorized software.	☐ Management does not have the ability to perform security monitoring,.

TLP_CLEAR_Joint_G...

Secureworks (Taegis) SIEM

Thursday, September 5, 2024 6:47 AM

In Secureworks (Taegis) SIEM, the goal is to detect security threats, maintain compliance, and ensure that your environment is properly secured. The platform provides threat intelligence, monitoring, and reporting on critical security events. To maximize its capabilities, you should run reports that focus on key security metrics, threat detection, and compliance.

Here are the most essential reports you should run in Secureworks SIEM:

1. User Authentication and Logon Activity

- Purpose: Track user logons and authentication attempts to detect potential unauthorized access or insider threats.
- What to check:
  - Successful and failed login attempts
  - Logins from unusual or unauthorized IP addresses
  - Failed login attempts followed by a successful login (indicating a potential brute-force attack)
  - Privileged account logon events

2. Privileged User Monitoring

- Purpose: Track the activity of privileged users (e.g., administrators) to detect potential misuse or unauthorized access.
- What to check:
  - Privileged user login attempts and activity
  - Changes to administrative groups (e.g., Domain Admins)
  - Sensitive command execution or configuration changes

3. Suspicious or Unauthorized Access Attempts

- Purpose: Detect and track attempts to gain unauthorized access to sensitive systems or data.
- What to check:
  - Access attempts to restricted systems or files
  - Multiple failed login attempts followed by a success (possible brute-force)
  - Unauthorized privilege escalation attempts

4. File Integrity Monitoring

- Purpose: Detect any unauthorized changes to critical files, configurations, or directories.
- What to check:
  - File changes in sensitive directories (e.g., configuration files, system files)
  - New file creation in restricted areas
  - Unauthorized changes to key system configurations

5. Malware and Threat Detection

- Purpose: Identify and monitor any malware-related activity within your environment.
- What to check:
  - Malware detection alerts (from endpoint detection tools or antivirus solutions)
  - Execution of suspicious or unauthorized processes
  - Indicators of compromise (IoCs), such as communication with known malicious IPs or domains
  - Files dropped by malware or suspicious binaries

6. Network Traffic Monitoring

SolarWinds Security Event Manager (SEM)

Thursday, September 5, 2024 6:48 AM

In SolarWinds Security Event Manager (SEM), running the right reports is crucial for effective monitoring, compliance, and security incident response. Here are some of the best reports to run in SolarWinds SEM:

1. User Login Activity Reports

- Purpose: Track successful and failed login attempts, including details about the user, the device, and time of access. Helps identify unauthorized access attempts or suspicious behavior.
- Examples:
  - Failed Login Attempts Report
  - Successful Logins by User

2. Privilege Use Reports

- Purpose: Monitor actions performed by privileged users to ensure that only authorized personnel are making changes. Critical for detecting misuse of admin accounts.
- Examples:
  - Privileged Account Usage
  - Administrative Changes Report

3. File Integrity Monitoring (FIM) Reports

- Purpose: Track file changes across critical systems to detect unauthorized modifications, deletions, or creations of sensitive files.
- Examples:
  - File Access and Changes Report
  - Configuration File Integrity Report

4. Security Events and Incident Detection

- Purpose: Identify suspicious activities, including malware detection, potential exploits, or other cybersecurity threats. These reports help in proactive security management.
- Examples:
  - Malware Detection Report
  - Intrusion Detection Activity Report

5. Compliance Reports

- Purpose: Meet regulatory requirements by running pre-built compliance reports that align with standards like PCI DSS, HIPAA, SOX, or GDPR.
- Examples:
  - PCI DSS Compliance Report
  - HIPAA Compliance Report
  - GDPR Activity Monitoring Report

6. Audit Trail Reports

- Purpose: Track changes to SEM configurations or rule sets. These reports are crucial for maintaining the integrity of SEM and ensuring proper change management.
- Examples:
  - SEM Configuration Change Report
  - Audit Log Activity Report

7. Event Correlation and Alerts Report

- Purpose: Analyze events that have triggered specific correlation rules. This is useful for identifying patterns and automating incident detection.
- Examples:
  - Event Correlation Report
  - Triggered Alerts Report

8. Network Device Monitoring Reports

- Purpose: Keep track of security-related events on network devices such as routers, switches, and firewalls.
- Examples:
  - Firewall Access and Denied Traffic Report
  - Network Device Security Events Report

9. Endpoint Activity Monitoring Reports

- Purpose: Monitor suspicious activity at the endpoint level, such as USB device usage, application activity, or remote desktop activity.
- Examples:
  - USB Device Usage Report
  - Application Execution Report
  - Remote Desktop Logins Report

10. SIEM Performance and Health Reports

- Purpose: Ensure SEM is running optimally by monitoring performance metrics, such as event collection, log storage, and system health.
- Examples:
  - Event Collection Summary
  - SEM Health Monitoring Report

11. Firewall and VPN Activity Reports

- Purpose: Monitor firewall traffic, VPN access, and policy changes to detect unauthorized access or unusual activity.
- Examples:
  - Firewall Activity Report
  - VPN Access Report

These reports can be customized further based on your specific use cases, compliance requirements, or security policies.

DarkTrace

Wednesday, September 18, 2024 2:02 PM

1. Initial Network Baseline and Learning Period

- **Allow the Learning Phase**: Once deployed, Darktrace needs time to learn the "normal" behavior patterns of your network, including common traffic patterns, user behaviors, and device communications. The learning period is crucial for identifying deviations that could indicate malicious activities.
- **Ensure Comprehensive Network Visibility**: Make sure Darktrace is integrated with all network segments to monitor both internal and external traffic. Deploy sensors across critical points like internet gateways, VPN access points, data centers, cloud services, and external-facing servers.
- **Incorporate Threat Feeds**: Integrate Darktrace with external threat intelligence feeds (e.g., known bad IPs or indicators of compromise) to enhance the detection of known external threats.

2. Set Up External Threat Detection Policies

- **Focus on External-Facing Assets**: Prioritize monitoring of external-facing assets, such as web servers, firewalls, email gateways, and VPN concentrators. Configure Darktrace to focus on unusual activity targeting these systems, which are often the entry point for penetration attempts.
- **Anomaly Detection on External Traffic**: Ensure Darktrace is tuned to detect unusual external traffic patterns, such as:
    - Unexpected connections from new or rare geolocations.
    - Repeated failed authentication attempts (brute force attacks).
    - Scanning activities (e.g., port scans or reconnaissance).
    - Sudden spikes in traffic to sensitive systems.
- **Unusual Protocol Use**: Darktrace can detect strange use of protocols (such as tunneling IPv6 over IPv4 or the use of uncommon ports) and attempts to exfiltrate data via unusual channels.

3. Custom Threat Models for External Penetration

- **Configure Darktrace's Threat Model Customization**: Tailor threat models specific to your environment for external penetration attempts:
    - **Web-Based Attacks**: Set up models to detect **SQL injection, cross-site scripting (XSS)**, and other web-based attacks targeting public-facing web servers.
    - **DNS Tunneling and C2 Communications**: Detect DNS queries used in **DNS tunneling** or suspicious outbound traffic to command-and-control (C2) servers.
    - **Fileless Malware and Exploitation Attempts**: Monitor for **suspicious memory injections**, **PowerShell usage**, and **unusual shell commands**, which could be part of exploitation techniques.

4. Integrate with Existing Security Controls

- **Firewall and IDS/IPS Integration**: Ensure Darktrace works in tandem with your firewalls, intrusion detection/prevention systems (IDS/IPS), and SIEMs. Use the anomaly detection capabilities to send logs and alerts directly to your firewall, blocking malicious IPs or suspicious traffic.
- **Web Application Firewall (WAF) Integration**: If you have a WAF, configure Darktrace to flag suspicious traffic patterns like web-based exploitation or penetration attempts, which can automatically trigger rules in the WAF to block attacks.
- **Log Correlation**: Feed Darktrace's alerts into your SIEM or a centralized logging platform for correlation with logs from other security appliances, improving the accuracy of detection and response.

5. Enable Autonomous Response with Antigena

- **Configure Darktrace Antigena**: Activate Darktrace **Antigena** for autonomous response capabilities. Antigena can intelligently interrupt malicious connections, stop lateral movement, or block traffic to malicious external destinations in real-time without manual intervention. Antigena can:
    - Quarantine affected devices attempting to communicate with suspicious IPs.
    - Block unusual outgoing traffic or unauthorized attempts to access external resources.
    - Temporarily restrict network privileges of compromised devices to contain the threat.

6. Monitor and Block Unauthorized External Connections

- **Identify Suspicious External IPs**: Configure Darktrace to monitor and flag any unusual or unauthorized external connections, such as:
    - Connections to known malicious IPs, Tor exit nodes, or blacklisted IPs.
    - Unusual outbound traffic to rarely-used geolocations.
    - Connections to newly registered domains, which could be linked to phishing or command-and-control.
- **Block Malicious IPs or Domains**: Automatically block or alert on any communication attempts with blacklisted IPs or domains that are commonly used for malware distribution or C2 communications.

7. Incident Response Playbooks

- **Develop Response Playbooks**: Create incident response playbooks within Darktrace for external penetration detection, ensuring quick response to suspicious activities. Playbooks should define steps for:
    - Investigating alerts related to reconnaissance or exploitation attempts.
    - Isolating affected systems automatically or manually.
    - Communicating with relevant teams (e.g., IT, security operations) for timely resolution.
- **Automated Alerting**: Set up real-time alerts for key personnel when Darktrace detects external penetration attempts or anomalous behavior patterns that could indicate an attack in progress.

8. Enable Traffic Monitoring and Forensics

- **Network Traffic Analysis**: Leverage Darktrace's **traffic mirroring** and **flow analysis** to continuously monitor network traffic and identify any anomalies in real-time. External penetration attempts often involve unusual inbound or outbound traffic patterns that can be flagged early.
- **Forensics and Threat Hunting**: Use Darktrace for retrospective analysis of suspicious activity. Regularly review alerts related to external penetration attempts for deeper analysis and incident forensics.

9. Testing and Tuning

- **Regular Penetration Testing**: Conduct penetration tests regularly to assess Darktrace's ability to detect and respond to external penetration attempts. Use these tests to fine-tune threat models and improve detection accuracy.
- **Threat Simulations**: Use breach-and-attack simulation tools to test Darktrace's responsiveness to various attack techniques, such as exploiting vulnerabilities in external services or attempting data exfiltration.

10. Continuous Learning and Updates

- **Adaptive Machine Learning**: Leverage Darktrace's adaptive machine learning to continuously refine its understanding of normal network behavior, improving its ability to detect sophisticated penetration attempts as your environment evolves.
- **Regular Updates**: Ensure Darktrace is kept up-to-date with the latest threat intelligence feeds and software updates to maximize its effectiveness in detecting new and emerging external threats.

Questions

Thursday, October 10, 2024 4:03 PM

Step 1: Understand the Requirements

1. Review Guidelines and Standards

- Q1.1: Have the relevant guidelines, such as NIST SP 800-137, CIS Controls, and the FFIEC IT Examination Handbook, been reviewed and understood?
- Q1.2: Does the organization ensure compliance with these guidelines for each CORE+ statement under Stmt 17?

2. Identify Key Assets

- Q2.1: Have key assets, such as firewalls, IDS/IPS, SIEM tools, network devices, and wireless access points, been identified for monitoring anomalous activity?
- Q2.2: Are these assets regularly reviewed and updated in the asset inventory to ensure coverage in the monitoring processes?

Step 2: Documentation Review

1. Review Security Policies and Procedures

- Q3.1: Are there documented security policies and procedures for monitoring network traffic, log collection, and event alerting?
- Q3.2: Are these policies up-to-date and aligned with regulatory requirements and emerging threats?
- Q3.3: Do the procedures specifically cover each component listed under Stmt 17?

Step 3: System Configuration Validation

1. Monitoring Incoming and Outgoing Network Traffic (Stmt 17.1 & 17.2)

- Q4.1: Are network monitoring tools (e.g., IDS/IPS, firewalls) configured to monitor both incoming and outgoing traffic?
- Q4.2: Are network traffic logs being generated, stored, and reviewed regularly?

2. Monitoring for Insider Malicious Activity (Stmt 17.3)

- Q5.1: Are tools such as user behavior analytics (UBA) used to monitor insider threats?
- Q5.2: Are alerts generated for anomalous insider activities, and are they promptly reviewed?

3. Logs Collected from Key Systems and Analyzed (Stmt 17.4 & 17.5)

- Q6.1: Are logs collected from critical systems like servers, firewalls, and endpoint security solutions?
- Q6.2: Is there a documented process for regular log analysis, and are past analysis reports reviewed?

4. Centralized Security Event Alerting and Logging (Stmt 17.6)

- Q7.1: Is a SIEM or an equivalent tool used for centralized log collection and correlation?
- Q7.2: Does the configuration of the SIEM ensure coverage of all enterprise assets?

5. Tuning Security Event Alerting Thresholds (Stmt 17.7)

- Q8.1: Is there a documented process for tuning alert thresholds in the SIEM?
- Q8.2: Is tuning performed at least monthly or more frequently as required?

6. Port Monitoring (Stmt 17.8)

- Q9.1: Are port monitoring tools in place to detect unauthorized network

connections?
- Q9.2: Is there a process to validate the configuration of these tools periodically?

7. Controls Over Wired and Wireless Networks (Stmt 17.9)
- Q10.1: Are NAC solutions implemented for wired and wireless networks to ensure only authorized devices connect?
- Q10.2: Is the configuration reviewed to ensure compliance with security standards?

8. Host-Based Intrusion Detection (Stmt 17.10)
- Q11.1: Is a host-based IDS deployed and actively monitoring enterprise assets?
- Q11.2: Are alerts generated by the IDS monitored and responded to effectively?

9. Traffic Filtering Between Network Segments (Stmt 17.11)
- Q12.1: Are traffic filtering mechanisms (e.g., firewalls, VLANs) in place between network segments?
- Q12.2: Are filtering rules reviewed and documented for appropriateness?

10. Application Layer Filtering (Stmt 17.12)
- Q13.1: Is an application layer filtering solution (e.g., proxy or firewall) deployed?
- Q13.2: Are rules configured to filter traffic at the application layer reviewed periodically?

11. Encryption on Wireless Networks (Stmt 17.13)
- Q14.1: Are encryption protocols (e.g., WPA2, WPA3) configured for wireless networks?
- Q14.2: Is the encryption configuration reviewed to ensure it is correctly implemented?

12. Wireless Network Segmentation (Stmt 17.14)
- Q15.1: Are wireless networks segmented to separate guest access from internal access?
- Q15.2: Are network diagrams reviewed to confirm proper segmentation?

13. Authentication Standards for Wireless Networks (Stmt 17.15)
- Q16.1: Are strong authentication mechanisms like 802.1x used for wireless networks?
- Q16.2: Are complex passwords and authentication protocols enforced and validated?

Step 4: Interview Relevant Personnel

1. Speak with IT and Security Teams
- Q17.1: Are personnel responsible for network monitoring, log analysis, and incident response aware of and following the documented procedures?
- Q17.2: Do these personnel participate in regular training and awareness programs related to their monitoring roles?

Step 5: Testing and Validation

1. Conduct Simulated Attacks
- Q18.1: Are penetration tests or red team exercises conducted to simulate attacks and insider threats?
- Q18.2: Is the effectiveness of monitoring systems evaluated based on the detection of these simulated activities?

2. Review Logs and Alerts
- Q19.1: Is there a sample log review process to validate the detection of anomalous activities?
- Q19.2: Are alerts reviewed for accuracy, and are actions taken documented

properly?

3. Assess Tuning Effectiveness

- Q20.1: Are tuning practices reviewed for effectiveness, focusing on the rate of false positives and the detection speed for real threats?
- Q20.2: Is there a documented process to adjust tuning practices based on testing outcomes?

Step 6: Reporting

1. Document Findings

- Q21.1: Are findings from the validation process documented in a detailed report?
- Q21.2: Are gaps or weaknesses identified, and are they clearly outlined with recommendations?

2. Recommendations

- Q22.1: Are recommendations provided to address any identified gaps or weaknesses in the monitoring process?
- Q22.2: Are follow-up actions assigned and tracked to ensure continuous monitoring and improvement?

Answers

Thursday, October 10, 2024 4:05 PM

Step 1: Understand the Requirements

1. Review Guidelines and Standards

- **Positive Response**: The relevant guidelines (e.g., NIST SP 800-137, CIS Controls, FFIEC IT Examination Handbook) have been reviewed, and the organization ensures full compliance with these guidelines for each CORE+ statement.
- **Negative Response**: The guidelines have not been reviewed or the organization does not have a process in place to ensure compliance for each CORE+ statement.

2. Identify Key Assets

- **Positive Response**: All key assets such as firewalls, IDS/IPS, SIEM tools, network devices, and wireless access points have been identified, documented, and are reviewed regularly.
- **Negative Response**: Key assets are not identified or documented, or there is no regular review process for these assets.

Step 2: Documentation Review

1. Review Security Policies and Procedures

- **Positive Response**: Security policies and procedures for monitoring network traffic, log collection, and event alerting are well-documented, up-to-date, and cover all necessary components.
- **Negative Response**: The organization lacks documented procedures, or existing policies are outdated and do not adequately cover the required components.

Step 3: System Configuration Validation

1. Monitoring Incoming and Outgoing Network Traffic (Stmt 17.1 & 17.2)

- **Positive Response**: Network monitoring tools are configured correctly to monitor all traffic, and logs are generated, stored, and reviewed on a regular schedule.
- **Negative Response**: Monitoring tools are either not configured properly or do not monitor both incoming and outgoing traffic. Logs are not consistently generated or reviewed.

2. Monitoring for Insider Malicious Activity (Stmt 17.3)

- **Positive Response**: User behavior analytics (UBA) tools are actively monitoring for insider threats, and alerts are generated and reviewed in a timely manner.
- **Negative Response**: No tools or inadequate tools are in place to monitor insider activity, or alerts are not consistently generated or reviewed.

3. Logs Collected from Key Systems and Analyzed (Stmt 17.4 & 17.5)

- **Positive Response**: Logs are consistently collected from critical systems, and there is a documented process for regular log analysis, with past reports reviewed for thoroughness.
- **Negative Response**: Logs are not collected from all critical systems, or the organization lacks a documented process for log analysis.

4. Centralized Security Event Alerting and Logging (Stmt 17.6)

- **Positive Response**: A SIEM or equivalent tool is in place, configured correctly, and covers all enterprise assets.

- **Negative Response**: No SIEM or equivalent tool is in use, or the tool is not configured to monitor all necessary assets.

5. Tuning Security Event Alerting Thresholds (Stmt 17.7)

- **Positive Response**: Alert thresholds are tuned at least monthly, and there is a clear, documented process for this activity.
- **Negative Response**: Alert thresholds are not tuned regularly, or no documented process exists for tuning them.

6. Port Monitoring (Stmt 17.8)

- **Positive Response**: Port monitoring tools are implemented and configured to detect unauthorized network connections, with periodic reviews conducted.
- **Negative Response**: Port monitoring tools are either absent or improperly configured, and there are no regular reviews.

7. Controls Over Wired and Wireless Networks (Stmt 17.9)

- **Positive Response**: Network Access Control (NAC) solutions are implemented and ensure only authorized devices connect. Regular configuration reviews are conducted.
- **Negative Response**: NAC solutions are not implemented or improperly configured, or configuration reviews are not conducted.

8. Host-Based Intrusion Detection (Stmt 17.10)

- **Positive Response**: Host-based IDS is deployed across enterprise assets, actively monitors, and generates alerts that are promptly acted upon.
- **Negative Response**: Host-based IDS is either not deployed or does not generate alerts as required, or alerts are not reviewed.

9. Traffic Filtering Between Network Segments (Stmt 17.11)

- **Positive Response**: Effective traffic filtering mechanisms (e.g., firewalls, VLANs) are in place and configured correctly. Rules are reviewed periodically for effectiveness.
- **Negative Response**: Inadequate traffic filtering mechanisms exist, or filtering rules are not properly configured or reviewed.

10. Application Layer Filtering (Stmt 17.12)

- **Positive Response**: An application layer filtering solution is in place with appropriate rules configured and regularly reviewed.
- **Negative Response**: No application layer filtering solution is in place, or rules are outdated or not reviewed regularly.

11. Encryption on Wireless Networks (Stmt 17.13)

- **Positive Response**: Wireless networks use up-to-date encryption protocols (e.g., WPA2, WPA3) with configurations validated for proper implementation.
- **Negative Response**: Encryption is either not used or is improperly configured, and no validation processes exist.

12. Wireless Network Segmentation (Stmt 17.14)

- **Positive Response**: Wireless networks are appropriately segmented, and network diagrams confirm segmentation is in place.
- **Negative Response**: Wireless networks are not segmented properly, or diagrams do not accurately reflect network segmentation.

13. Authentication Standards for Wireless Networks (Stmt 17.15)

- **Positive Response**: Strong authentication mechanisms (e.g., 802.1x) are implemented, with complex passwords enforced and validated.
- **Negative Response**: Weak or absent authentication mechanisms are in place, or password protocols are not enforced.

Step 4: Interview Relevant Personnel

1. Speak with IT and Security Teams

- **Positive Response**: IT and security personnel are knowledgeable, trained, and actively following documented procedures.
- **Negative Response**: Personnel lack awareness of procedures or have not received appropriate training.

Step 5: Testing and Validation

1. Conduct Simulated Attacks

- **Positive Response**: Penetration testing and red team exercises are conducted, and monitoring systems successfully detect these simulated threats.
- **Negative Response**: Tests are not conducted, or systems fail to detect simulated threats effectively.

2. Review Logs and Alerts

- **Positive Response**: Sample logs and alerts show effective detection and response to anomalous activities, with consistent documentation.
- **Negative Response**: Logs and alerts indicate failures in detection, or there is inadequate documentation of actions taken.

3. Assess Tuning Effectiveness

- **Positive Response**: Tuning practices effectively minimize false positives and maximize the speed and accuracy of threat detection.
- **Negative Response**: Tuning practices are either not reviewed or fail to improve detection accuracy, leading to a high rate of false positives.

Step 6: Reporting

1. Document Findings

- **Positive Response**: Findings are documented comprehensively, with all identified gaps clearly outlined and addressed in reports.
- **Negative Response**: Documentation is incomplete, and gaps are not clearly identified or addressed.

2. Recommendations

- **Positive Response**: Recommendations are clear, actionable, and based on findings. Follow-up actions are assigned and monitored.
- **Negative Response**: Recommendations are vague, unfeasible, or not acted upon, and follow-up actions are not tracked.

Checklist

Thursday, October 10, 2024 4:05 PM

Audit Checklist Template for Monitoring and Anomalous Activity Compliance

Audit Overview

- **Audit Title**: Monitoring and Anomalous Activity Compliance Audit
- **Date**: [Date]
- **Auditor Name**: [Auditor's Name]
- **Credit Union Name**: [Credit Union Name]
- **Audit Period**: [Start Date] to [End Date]

Section 1: Understanding the Requirements

#	Task	Description	Status (Yes/No)	Notes/Comments
1.1	Review Guidelines	Have the guidelines (NIST SP 800-137, CIS Controls, FFIEC IT Examination Handbook) been reviewed and understood?	[ ]	
1.2	Compliance Assurance	Does the organization ensure compliance with guidelines for each CORE+ statement under Stmt 17?	[ ]	
1.3	Identify Key Assets	Are key assets (e.g., firewalls, IDS/IPS, SIEM tools) identified and documented?	[ ]	
1.4	Asset Review	Are assets reviewed and updated regularly?	[ ]	

Section 2: Documentation Review

#	Task	Description	Status (Yes/No)	Notes/Comments
2.1	Policy Documentation	Are security policies and procedures documented for monitoring network traffic and log collection?	[ ]	
2.2	Policy Update Frequency	Are policies up-to-date and aligned with regulatory requirements?	[ ]	
2.3	Procedure Specificity	Do procedures cover each component listed under Stmt 17?	[ ]	

Section 3: System Configuration Validation

Stmt 17.1 & 17.2: Monitoring Network Traffic

#	Task	Description	Status (Yes/No)	Notes/Comments
3.1	Network Monitoring	Are network monitoring tools configured for both incoming and	[ ]	

		outgoing traffic?	
3.2	Log Generation	Are network traffic logs generated and stored properly?	[ ]

Stmt 17.3: Monitoring Insider Malicious Activity

#	Task	Description	Status (Yes/No)	Notes/Comments
3.3	UBA Tools	Are tools used to monitor insider threats (e.g., UBA tools) in place?	[ ]	
3.4	Alert Generation	Are alerts generated and promptly reviewed for insider threats?	[ ]	

Stmt 17.4 & 17.5: Log Collection and Analysis

#	Task	Description	Status (Yes/No)	Notes/Comments
3.5	Log Collection	Are logs collected from critical systems such as servers and firewalls?	[ ]	
3.6	Log Analysis Process	Is there a documented process for regular log analysis?	[ ]	

Stmt 17.6: Centralized Security Event Alerting

#	Task	Description	Status (Yes/No)	Notes/Comments
3.7	SIEM Implementation	Is a SIEM or equivalent tool used for centralized log collection?	[ ]	
3.8	SIEM Configuration	Does the SIEM cover all enterprise assets?	[ ]	

Stmt 17.7: Tuning Security Event Alerting Thresholds

#	Task	Description	Status (Yes/No)	Notes/Comments
3.9	Alert Tuning	Is there a documented process for tuning alert thresholds?	[ ]	
3.10	Frequency of Tuning	Is tuning performed at least monthly or as needed?	[ ]	

Section 4: Port Monitoring and Network Controls

Stmt 17.8: Port Monitoring

#	Task	Description	Status (Yes/No)	Notes/Comments
4.1	Port Monitoring Tools	Are port monitoring tools implemented and configured correctly?	[ ]	

Stmt 17.9: Controls Over Wired and Wireless Networks

#	Task	Description	Status	Notes/Com

			(Yes/No)	ments
4.2	NAC Solutions	Are NAC solutions in place for wired and wireless networks?	[ ]	

Section 5: Intrusion Detection and Filtering

Stmt 17.10: Host-Based Intrusion Detection

#	Task	Description	Status (Yes/No)	Notes/Comments
5.1	Host-Based IDS	Is a host-based IDS deployed and configured?	[ ]	

Stmt 17.11: Traffic Filtering Between Network Segments

#	Task	Description	Status (Yes/No)	Notes/Comments
5.2	Filtering Mechanisms	Are traffic filtering mechanisms (e.g., firewalls) in place and reviewed regularly?	[ ]	

Section 6: Wireless Network Security

Stmt 17.13: Encryption on Wireless Networks

#	Task	Description	Status (Yes/No)	Notes/Comments
6.1	Encryption Protocols	Are WPA2 or WPA3 encryption protocols in use for wireless networks?	[ ]	

Stmt 17.14: Wireless Network Segmentation

#	Task	Description	Status (Yes/No)	Notes/Comments
6.2	Network Segmentation	Are wireless networks segmented appropriately to separate guest access from internal networks?	[ ]	

Section 7: Personnel Awareness and Training

#	Task	Description	Status (Yes/No)	Notes/Comments
7.1	Staff Training	Are personnel responsible for monitoring trained and aware of procedures?	[ ]	

Section 8: Testing and Validation

#	Task	Description	Status (Yes/No)	Notes/Comments
8.1	Penetration Testing	Are penetration tests conducted to simulate attacks and validate monitoring?	[ ]	
8.2	Log Review	Are logs and alerts reviewed to ensure proper detection and response?	[ ]	

Section 9: Reporting and Recommendations

#	Task	Description	Status (Yes/No)	Notes/Comments
9.1	Documentation of Findings	Are findings documented comprehensively with clear recommendations?	[ ]	
9.2	Follow-Up Actions	Are follow-up actions assigned and tracked to ensure improvement?	[ ]	

Audit Summary

- **Total Tasks Completed**: [Total Completed/Total Tasks]
- **Comments/Recommendations**: [Detailed Findings and Recommendations]
- **Sign-Off**: [Auditor's Signature and Date]

Notes

Wednesday, September 18, 2024 1:56 PM