Clearnetwork USM – Unified Security Management – HIPAA Compliance

Any organization that transmits any health information in electronic form, including health plans, healthcare clearing houses, healthcare providers, and business associates of a covered entity, must comply with HIPAA.

Yet, according to the US Department of Health and Human Services, one of the top issues that organizations have is failure to sufficiently safeguard electronic protected health information. One of the big challenges is the number of security controls that organizations need to deploy, often requiring numerous security point products that are costly to procure and difficult to deploy and manage.

Clearnetwork USM is fully managed, and all data is fully analyzed by Clearnetwork's team of security analysts, who are also Alienvault Certified Engineers.

The following is a breakdown of what is provided with our USM service

- Asset Discovery and Inventory
- Vulnerability Assessment
- Intrusion Detection (IDS)
- File Integrity Monitoring (FIM)
- SIEM Event Correlation
- Log Management & Monitoring
- Behavioral Analysis
- Endpoint Detection and Response
- Integration with existing security systems

§164.308(a)(1) - Security Management Process

Implement policies and procedures to prevent, detect, contain, and correct security violations.

§164.308(a)(1)(ii)(A) - Risk Analysis

§164.308(a)(1)(ii)(D) - Information System Activity Review

- Asset discovery discovers assets running on-premises, and in cloud environments (including Azure, VMware, Hyper-V, AWS).
- Identifies systems susceptible to known vulnerabilities, and ranks them as 'high', 'medium' and 'low' risk to aid prioritization.

- Identifies patches or workarounds available to vulnerable systems.
- Identifies where security tools, such as antivirus and firewalls, have been disabled or have failed to start.
- Monitors access to and attempt to modify system and application binaries, configuration files, log files.
- Monitor user and administrator activities in cloud environments such as Azure and AWS, and within cloud applications such as Office 365.
- Continuously updated threat intelligence ensures that Clearnetwork USM is operating with the latest correlation directives, vulnerability signatures, IDS rules, reports, guided threat response and more.
- Aggregates, analyzes and archives logs and events from systems, applications and devices from across your on-premises and cloud environments.
- Identifies logon success and failures.
- Identifies privilege escalation attempts.
- Identifies unauthorized attempts to access or modify key logs.

§164.308(a)(3) - Workforce Security

Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information ..., and to prevent those workforce members who do not have access ... from obtaining access to electronic protected health information.

§164.308(a)(3)(ii)(A) - Authorization and/or Supervision

§164.308(a)(3)(ii)(C) - Termination Procedures

- Monitor access attempts to critical files and data, and alarm when unauthorized attempts are detected.
- Capture and monitor all login successes and failures to critical assets, particularly those containing electronic protected health information.
- Monitor for logon or access attempts from the accounts of users who have been de-provisioned.

§164.308(a)(4) - Information Access Management

Implement policies and procedures to prevent, detect, contain, and correct security violations.

§164.308(a)(4)(ii)(C) - Access Establishment and Modification

- Captures all user account creation and modification activities.
- Identifies logon success and failures.
- Identifies privilege escalation attempts.

§164.308(a)(5) - Security Awareness and Training

Procedures for monitoring log-in attempts and reporting discrepancies

§164.308(a)(5)(ii)(A) - Security Reminders

§164.308(a)(5)(ii)(B) - Protection from Malicious Software

§164.308(a)(5)(ii)(C) - Log-in Monitoring

§164.308(a)(5)(ii)(D) - Password Management

- Provision for automated updates of USM infrastructure whenever updates are made available.
- Continuously updated threat intelligence ensures that USM is operating with the latest correlation directives, vulnerability signatures, IDS rules, reports, guided threat response and more.
- Identifies systems susceptible to known vulnerabilities, or that may not have antivirus installed and/or operational.
- Identifies indicators of malware-based compromise, and enables orchestrated responses that can be automated or manually invoked to isolate infected systems and block malicious domains.
- Monitors and stores events from antivirus solutions that could indicate a compromise, or attempt to disable antivirus software.
- Monitors for changes to Office 365 policies including Information Management, and more.
- Continuously updated threat intelligence ensures that USM is operating with the latest correlation directives, vulnerability signatures, IDS rules, reports, guided threat response and more.
- Captures and enables monitoring of logon success and failures to systems, security devices, cloud environments, and more.
- Identifies where new user and administrator accounts are created and deleted.
- Monitors public and dark web sources for the trade or communication of stolen credentials.
- Identifies use of default system accounts on Windows machines.
- File Integrity Monitoring can detect changes and access to critical system and application files, and Windows Registry entries.

§1164.308(a)(6) - Security Incident Procedures

Implement policies and procedures to prevent, detect, contain, and correct security violations.

§164.308(a)(6)(ii) - Response and Reporting

- Correlates events to detects threats
- Generates alarms on threats, classifying them across a kill-chain taxonomy to inform the risk level of that threat.
- Enables threat investigation and provides context to determine the nature of the threat.

- Provides recommended incident response guidance to contain or remediate the threat.
- Enables labels to be applied to alarms.
- Security orchestration and response capabilities enable manual or automated incident response, driving actions with leading security and IT operations tools including Cisco Umbrella, Carbon Black, Palo Alto Firewalls, and more.
- Enables creation of incident tickets within popular solutions like ServiceNow, directly from within the USM console.
- Continuously updated threat intelligence ensures that USM is operating with the latest correlation directives, vulnerability signatures, IDS rules, reports, guided threat response and more.

§164.308(a)(7) - Contingency Plan

Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.

§164.308(a)(7)(ii)(E) - Applications and Data Criticality Analysis

- USM provides a fault resilient architecture that assures durability of all captured event and log data from your environments.

§164.312(a) - Access Control

Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights.

§164.312(a)(2)(iii) - Automated Logoff

§164.312(a)(2)(iv) - Encryption and Decryption

- Monitors for changes to Windows Group Policy and Office 365 policies that define automated logoff, session timeout, and access token timeout parameters.
- Monitors for changes to Windows Registry or application configuration files that define encryption settings for protected health information.

§164.312(b) - Audit Controls

Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.

- Monitors for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more.
- File Integrity Monitoring can detect modification attempts to applications or online storage containing electronic protected health information.
- Unified log collection, review and analysis, with triggered alarms for high risk systems.

§164.312(c)(1) - Integrity

Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.

§164.312(c)(2) - Audit Controls

- Monitors for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more.
- File Integrity Monitoring can detect modification attempts to applications or online storage containing electronic protected health information.

§164.312(e)(1) - Transmission Security

Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.

§164.312(e)(2)(i) - Integrity Controls

§164.312(e)(2)(ii) - Encryption

- Discover unauthorized communications, such as between untrusted networks and systems within the cardholder data environment.
- Monitors for changes to Office 365 policies including Data Leakage Protection (DLP), information management, and more.
- File Integrity Monitoring can detect modification attempts to applications or online storage containing electronic protected health information.
- Monitors for changes to Windows Group Policy and Office 365 policies that define automated logoff, session timeout, and access token timeout parameters.
- Monitors for changes to Windows Registry or application configuration files that define encryption settings for protected health information.